

BLOCKCHAIN for GOVERNMENT SERVICES

การใช้เทคโนโลยีบล็อกเชนสำหรับภาครัฐ

เวอร์ชัน 2.0 (มกราคม พ.ศ. 2564)



DGA
Digital Government Development Agency

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพว.)

Digital Government Development Agency (Public Organization) (DGA)

BLOCKCHAIN for GOVERNMENT SERVICES

การใช้เทคโนโลยีบล็อกเชนสำหรับภาครัฐ

เวอร์ชัน 2.0 (มกราคม พ.ศ. 2564)



บรรณาธิการบริหาร : ดร.ศักดิ์ เสกขุนทด

บรรณาธิการ : นายวิบูลย์ ภัทรพิบูล
นายพิสิษฐ์ ปิยะสุนทร

คณะผู้จัดทำ : ดร.มณฑา ชยากรวิกรม
นายเกียรติศักดิ์ วงศ์ประเสริฐ
นายสมมนัส เกตุผ่อง
นายชฎิล อินทร-นก
นายสถาปน พัฒนะคูหา

ฝ่ายศิลป์ และครีเอทีฟ : นายสุวินันท์ ฤกษ์สง่า
นายธามัน ศิริกุล
นางสาววริยา สรรคชา
นายวิรุฬห์ ดาราภัย

จัดทำโดย : สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

พิมพ์ครั้งที่ 2 : พ.ศ. 2564

จำนวน : 300 เล่ม

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพว.)

Digital Government Development Agency (Public Organization) (DGA)

อาคารบางกอกไทยทาวเวอร์ 108 ถนนรางน้ำ
แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ 10400

โทรศัพท์ : (+66) 0 2612 6000

โทรสาร : (+66) 0 2612 6011 , (+66) 0 2612 6012

Contact Center : (+66) 0 2612 6060

อีเมล : contact@dga.or.th



คำนำ

เทคโนโลยี Blockchain เป็นเทคโนโลยีที่เข้ามาขับเคลื่อนการพัฒนาเศรษฐกิจและสังคมโลกในยุคดิจิทัล ซึ่งได้รับความสนใจและทำการศึกษากันอย่างกว้างขวางทั้งในประเทศและต่างประเทศ นอกจากเทคโนโลยี Blockchain จะเข้ามาปฏิวัติโลกธุรกิจ และแวดวงการเงินการธนาคารแล้ว ยังมีบทบาทในการยกระดับการบริหารงานภาครัฐเพื่อเข้าสู่การเป็นรัฐบาลดิจิทัล (Digital Government) รวมถึงการเปลี่ยนวิถีชีวิตของประชาชนไปสู่ความสะดวกสบายมากขึ้นเช่นเดียวกับอิทธิพลของโลกออนไลน์ในขณะนี้ ดังนั้นนักวางแผน นักกลยุทธ์ ตลอดจนผู้กำหนดนโยบายภาครัฐ จึงควรตระหนักถึงอิทธิพล และผลกระทบของเทคโนโลยี Blockchain ที่จะเกิดขึ้นในอนาคตอันใกล้นี้ เพื่อเตรียมความพร้อมต่อโอกาสและความท้าทายในอนาคตที่จะทำให้ประเทศไทยมีความได้เปรียบ เมื่อเทคโนโลยี Blockchain ถูกนำมาใช้งานอย่างเต็มรูปแบบ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร. หรือ DGA มีภารกิจหลักที่สำคัญในการขับเคลื่อนรัฐบาลดิจิทัล โดยเฉพาะด้านการส่งเสริมและสนับสนุนการบูรณาการและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐ การเปิดเผยข้อมูลภาครัฐผ่านเทคโนโลยีดิจิทัล และเป็นศูนย์กลางการแลกเปลี่ยนทะเบียนข้อมูลดิจิทัลภาครัฐเพื่ออำนวยความสะดวกให้ประชาชนและการดำเนินงานของหน่วยงานภาครัฐ ดังนั้น Blockchain จึงเป็นเทคโนโลยีดิจิทัลที่สำคัญเหมาะสมในการนำมาใช้งานบริการภาครัฐ ในด้านการจัดเก็บข้อมูลภาครัฐ เนื่องจากมีคุณลักษณะที่มีความถูกต้องเที่ยงตรงของข้อมูล (Data Integrity) ความโปร่งใสในการเข้าถึงข้อมูล (Data Transparency) และมีความสามารถในการทำงานได้อย่างต่อเนื่องของระบบ (Availability) สามารถมาใช้ในการจัดเก็บข้อมูลภาครัฐ เป็นการเปิดโอกาสให้ประชาชน มีสิทธิเป็นเจ้าของข้อมูลของตนเองอย่างแท้จริง รวมไปถึงโอกาสในการเข้าถึงข้อมูลภาครัฐต่าง ๆ ง่ายขึ้น ซึ่ง สพร. ได้มีการนำเทคโนโลยี Blockchain มาพัฒนาเพื่อให้บริการแก่ภาครัฐและประชาชนในอนาคตอันใกล้นี้

และเพื่อส่งเสริมให้ทุกภาคส่วน “รู้ รับ ปรับใช้” เทคโนโลยีใหม่ได้อย่างต่อเนื่อง สพร. จึงได้จัดทำหนังสือ การใช้งานเทคโนโลยี Blockchain สำหรับภาครัฐ (Blockchain for Government Services) ฉบับภาษาไทยขึ้น เพื่อเผยแพร่องค์ความรู้เกี่ยวกับเทคโนโลยี Blockchain รวมถึงบทวิเคราะห์การประยุกต์ใช้เทคโนโลยี Blockchain โดยเนื้อหาในหนังสือแบ่งออกเป็น 3 ส่วนด้วยกัน ดังต่อไปนี้



การให้ความรู้พื้นฐานเกี่ยวกับหลักการทำงานของเทคโนโลยี Blockchain



การประยุกต์ใช้เทคโนโลยี Blockchain เพื่องานบริการภาครัฐ กรณีศึกษาต่างประเทศ



แนวคิดและหลักการประยุกต์ใช้เทคโนโลยี Blockchain สำหรับภาครัฐ ภายใต้บริบทของประเทศไทย

คณะผู้จัดทำหวังเป็นอย่างยิ่งว่าหนังสือเล่มนี้ จะเป็นประโยชน์ต่อสาธารณชน ทั้งภาคเอกชน และประชาชนที่สนใจ รวมถึงหน่วยงานภาครัฐสามารถนำไปประยุกต์ใช้เพื่อยกระดับคุณภาพบริการให้มีประสิทธิภาพและทันสมัย ถูกใจประชาชนมากยิ่งขึ้น สำหรับหนังสือฉบับนี้ สพร. ได้จัดทำเป็น e-Magazine แจกฟรี สามารถดาวน์โหลดได้ที่เว็บไซต์ www.dga.or.th



คณะผู้จัดทำ

สารบัญ

คำนำ	02
อภิธานศัพท์	13
บทที่ 1	
บทนำ	18
เทคโนโลยี Blockchain	19
หลักการทำงานของเทคโนโลยี Blockchain	22
องค์ประกอบของเทคโนโลยี Blockchain	25
ประเภทของ Blockchain	37
คุณลักษณะพื้นฐานที่สำคัญของเทคโนโลยี Blockchain	45
• ความถูกต้องเที่ยงตรงของข้อมูล (Data Integrity)	45
• ความโปร่งใสในการเข้าถึงข้อมูล (Data Transparency)	45
• ความสามารถในการทำงานได้อย่างต่อเนื่องของระบบ (Availability)	46
เกณฑ์การพิจารณาเลือกใช้เทคโนโลยี Blockchain	47
รูปแบบการประยุกต์ใช้เทคโนโลยี Blockchain	48
• เงินดิจิทัล (Cryptocurrency)	51
• บริการพิสูจน์ทราบ (Proof of Services)	51
• สัญญาอัจฉริยะ (Smart Contract)	53
• ระบบ/บริการอัตโนมัติ (Decentralized Autonomous Systems/ Services)	58
บทที่ 2	
การประยุกต์ใช้เทคโนโลยี Blockchain	60
เพื่องานบริการภาครัฐ กรณีศึกษาต่างประเทศ	
การประยุกต์ใช้เทคโนโลยี Blockchain เพื่องานบริการภาครัฐ กรณีศึกษาต่างประเทศ	61
ประโยชน์ของการนำเทคโนโลยี Blockchain มาใช้สำหรับงานบริการภาครัฐ	70

ข้อจำกัดของการนำเทคโนโลยี Blockchain มาใช้เพื่องานบริการภาครัฐ	74
รูปแบบการประยุกต์ใช้เทคโนโลยี Blockchain เพื่องานบริการภาครัฐ	80
• การพิสูจน์ตัวตน (Identity Management)	82
• การบริหารจัดการการจัดเก็บข้อมูล (Data Record Management)	86
• การติดตามธุรกรรม (Transaction Traceability)	93
ปัจจัยความสำเร็จในการประยุกต์ใช้เทคโนโลยี Blockchain	105
เพื่องานบริการภาครัฐ	
• การจัดตั้งคณะทำงานแห่งชาติ (The National Blockchain Council)	106
• การสร้างระบบนิเวศของเทคโนโลยี Blockchain (Blockchain Ecosystem)	111
• การสร้างการกำกับดูแลการใช้งานเทคโนโลยี Blockchain (Blockchain Governance)	111
• การกำหนดมาตรฐานเกี่ยวกับเทคโนโลยี Blockchain	113
• การพัฒนาบุคลากรที่มีความรู้ความสามารถด้านเทคโนโลยี Blockchain	117

บทที่ 3

แนวคิดและหลักการประยุกต์ใช้เทคโนโลยี Blockchain	121
สำหรับภาครัฐ ภายใต้บริบทของประเทศไทย	
หลักการและเหตุผลการประยุกต์ใช้เทคโนโลยี Blockchain	122
สำหรับภาครัฐไทย	
การประยุกต์ใช้เทคโนโลยี Blockchain เพื่อการบูรณาการบริการ	138
และแลกเปลี่ยนข้อมูลภาครัฐ	
กรณีศึกษาการจัดทำระบบต้นแบบ e-Referral โดยใช้เทคโนโลยี Blockchain	152

เอกสารแนบท้าย 1	176
------------------------	-----

สารบัญภาพ

รูปภาพที่ 1

ระบบแบบ
Centralised,
Decentralised
และ Distributed

19

รูปภาพที่ 2

การเชื่อมโยงข้อมูล
ของเทคโนโลยี Blockchain

20

รูปภาพที่ 3

หลักการทำงาน
ของเทคโนโลยี
Blockchain

23

รูปภาพที่ 4

องค์ประกอบของเทคโนโลยี
Blockchain

25

รูปภาพที่ 5

โครงสร้างการเชื่อมโยง
Block

26

27 รูปภาพที่ 6

โครงสร้างภายใน Block
ของ Bitcoin

30 รูปภาพที่ 7

ตัวอย่างการแสดงผล Block
Information ของ Bitcoin

31 รูปภาพที่ 8

หลักการ Hash ข้อมูลชุดใหญ่
โดยใช้รูปแบบ Hash Tree

37 รูปภาพที่ 9

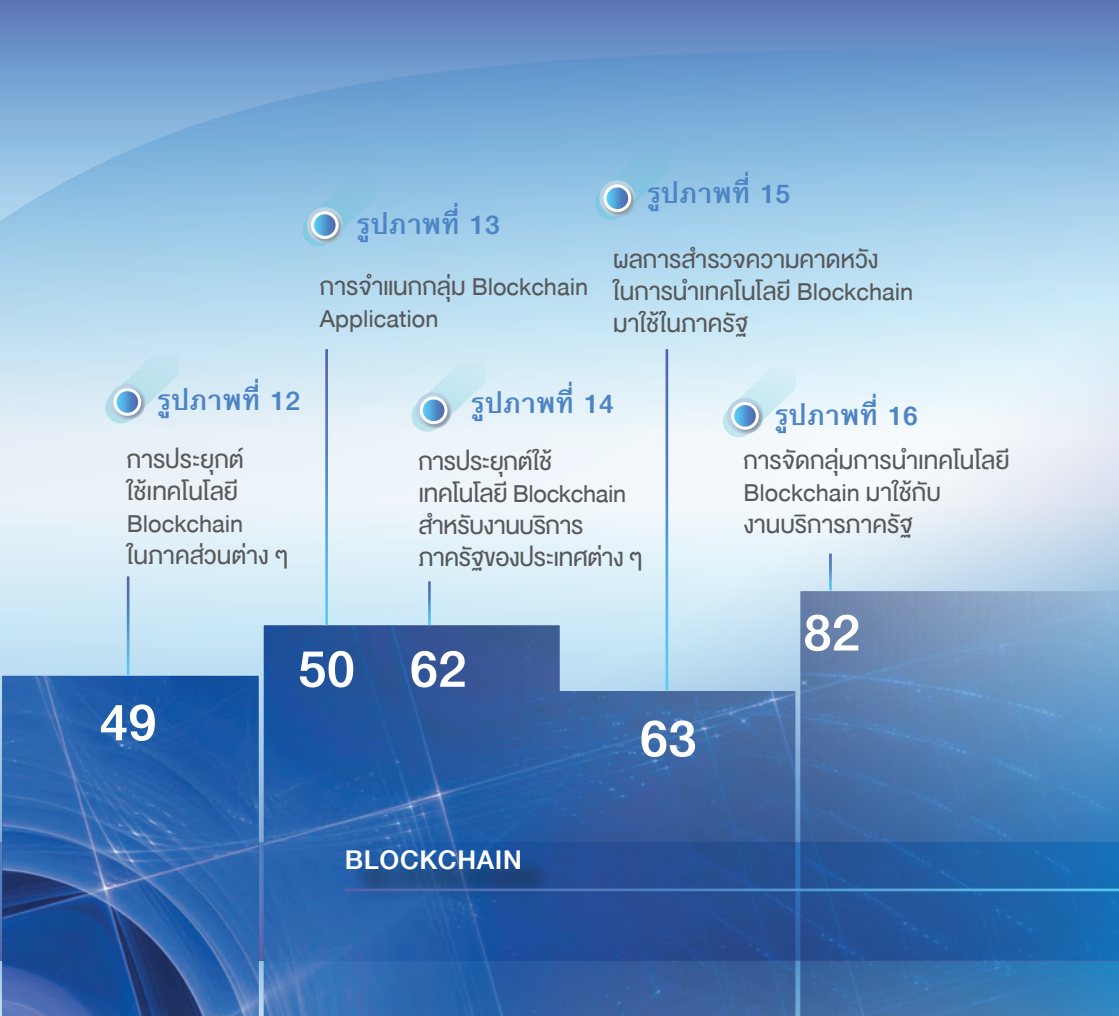
Public Blockchain

39 รูปภาพที่ 10

Private Blockchain

47 รูปภาพที่ 11

กระบวนการตัดสินใจก่อน
การนำเทคโนโลยี Blockchain
มาใช้งาน



84 รูปถ่ายที่ 17
ระบบยืนยันและพิสูจน์ตัวตนบนเทคโนโลยี Blockchain

98 รูปถ่ายที่ 18
ภาพขั้นตอนและกระบวนการของการขออนุญาตหนังสือค้าประกันแบบกระดาษรูปแบบเดิม

99 รูปถ่ายที่ 19
ภาพการเปิดตัว บิซีไอ ณ ธนาคารแห่งประเทศไทย

100 รูปถ่ายที่ 20
ภาพขั้นตอนและกระบวนการของการขออนุญาตหนังสือค้าประกันอิเล็กทรอนิกส์ผ่านระบบบล็อกเชน

101 รูปถ่ายที่ 21
รูปแสดงโครงสร้างโดะแกรมของเน็ตเวิร์คบล็อกเชนและเชื่อมต่อ

103 รูปถ่ายที่ 22
ภาพการเปิดตัวบริการหนังสือค้าประกันอิเล็กทรอนิกส์บนระบบ e-GP ผ่านเทคโนโลยีบล็อกเชน

สารบัญภาพ (ต่อ)

รูปภาพที่ 23

ปัจจัยความสำเร็จในการประยุกต์ใช้เทคโนโลยี Blockchain สำหรับงานบริการภาครัฐ

105

รูปภาพที่ 24

วิสัยทัศน์รัฐบาลดิจิทัล

123

128

รูปภาพที่ 25

แนวโน้มเทคโนโลยีที่สำคัญสำหรับการพัฒนารัฐบาลดิจิทัล

รูปภาพที่ 26

ระบบบูรณาการการให้บริการภาครัฐโดยใช้ Enterprise Service Bus (ESB)

139

รูปภาพที่ 27

การเชื่อมโยงบูรณาการการให้บริการภาครัฐโดยใช้เทคโนโลยี Blockchain

142

144 รูปภาพที่ 28

องค์ประกอบทางเทคนิคการบูรณาการงานบริการภาครัฐบนเทคโนโลยี Blockchain

147 รูปภาพที่ 29

แสดงระบบนิเวศการให้บริการหน่วยงานภาครัฐ

150 รูปภาพที่ 30

แผนภาพจำลองขั้นตอนการขออนุญาตเข้ามาในราชอาณาจักรชั่วคราวเพื่อเข้ารับการรักษาพยาบาล

156 รูปภาพที่ 31

ภาพรวมสถาปัตยกรรมระบบต้นแบบ e-Referral บนเทคโนโลยี Blockchain

159 รูปภาพที่ 32

รายละเอียดการออกแบบระบบต้นแบบ e-Referral บนเทคโนโลยี Blockchain

163 รูปภาพที่ 33

แผนภาพแสดงขั้นตอนการส่งต่อผู้ป่วยระหว่างโรงพยาบาล

รูปภาพที่ 34

ตัวอย่างการเขียนโปรแกรม
ของการบริหารสิทธิ์
ในการเข้าถึงและ
ใช้งานข้อมูลผู้ป่วย
โดยใช้ Smart Contract

165

รูปภาพที่ 35

โรงพยาบาลต้นทาง
สามารถส่งต่อผู้ป่วย
ผ่านหน้าจอร์บบ e-Referral

166

รูปภาพที่ 36

โรงพยาบาลปลายทาง
สามารถส่งคำขอส่งต่อผู้ป่วย
ผ่านหน้าจอร์บบ e-Referral

167

รูปภาพที่ 37

โรงพยาบาลปลายทาง
สามารถเข้าดูข้อมูลผู้ป่วย
ในระบบ 13 แฟ้มได้

167

รูปภาพที่ 38

โรงพยาบาลปลายทาง
สามารถรองรับ ปฏิเสธ
หรือขอเลื่อนเวลาการส่งต่อ
ผู้ป่วยได้

168

for GOVERNMENT SERVICES

168 รูปภาพที่ 39

ตัวอย่าง Log การส่งต่อผู้ป่วย
ของระบบ e-Referral

169 รูปภาพที่ 40

หน้าจอ Dashboard
แสดงรายงานต่าง ๆ
ของระบบ e-Referral

169 รูปภาพที่ 41

หน้าจอสำหรับ
การ Performance Monitoring ,
Report และ Throughput
ใน Component ต่าง ๆ
ของระบบ Hyperledger
Blockchain

สารบัญตาราง

BLOCKCHAIN
for GOVERNMENT SERVICES



ตารางที่ 1

ตารางเปรียบเทียบ
คุณสมบัติของเทคโนโลยี
Blockchain
ในแต่ละประเภท

41



ตารางที่ 2

ตารางแสดงการประยุกต์
ใช้เทคโนโลยี Blockchain
สำหรับงานบริการ
ภาครัฐในต่างประเทศ

81



ตารางที่ 3

ตารางสรุป
ความเป็นไปได้
ในการประยุกต์ใช้
เทคโนโลยี Blockchain
สำหรับงานบริการ
ภาครัฐของประเทศไทย

130

อภิธานศัพท์

Blockchain

เทคโนโลยีการจัดเก็บข้อมูลแบบ Shared Database หรือที่รู้จักกันในชื่อ “Distributed Ledger Technology (DLT)” โดยเป็นรูปแบบการบันทึกข้อมูลที่รับประกันความปลอดภัยว่าข้อมูลที่ถูกบันทึกไปก่อนหน้านี้ไม่สามารถที่จะเปลี่ยนแปลงหรือแก้ไข ซึ่งทุกผู้ใช้งานจะได้เห็นข้อมูลชุดเดียวกันทั้งหมด โดยใช้หลักการ Cryptography และความสามารถของ Distributed Computing เพื่อสร้างกลไกความน่าเชื่อถือ

Block

ชุดบรรจุข้อมูล แบ่งออกเป็น 2 ส่วน คือ ส่วนของข้อมูลต่าง ๆ ที่ต้องการบรรจุลงใน Block เรียกว่า Block Data เช่น ข้อมูลการทำธุรกรรมต่าง ๆ และส่วนของ Block Header ที่ใช้เก็บข้อมูลประจำ Block นั้น ๆ ได้แก่ หมายเลข Block, ค่า Nounce, ค่า Previous Hash และค่า Current Hash เป็นต้น

Nonce

ค่าที่ถูกสุ่มขึ้นมา เพื่อใช้ในการค้นหาค่า Hash ของ Block ซึ่งจะต้องเป็นไปตามกฎของระบบที่ได้กำหนดไว้ โดยค่า Hash ที่ได้นั้นจะต้องมีค่าต่ำกว่าค่า Target หรืออีกชื่อหนึ่งคือ ค่า Difficulty นั้นเอง ซึ่งส่วนใหญ่มักใช้ในการออกแบบโครงสร้าง Block ของ Bitcoin

Previous Hash

ค่า Current Hash ของ Block ก่อนหน้า ซึ่งเปรียบได้กับค่า Digital Signature ของ Block ก่อนหน้าโดยจะถูกจัดเก็บอยู่ในโครงสร้างของ Block ถัดไปเสมอ และหากมีการแก้ไขข้อมูลใน Block ก่อนหน้าจะทำให้ค่า Hash ของ Block ไม่เท่ากัน ทั้งนี้ในการออกแบบโครงสร้าง Block แต่ละแพลตฟอร์มอาจมีการใช้ชื่อเรียกที่แตกต่างกันออกไป

Current Hash

ค่า Hash ของข้อมูลทั้งหมดใน Block นั้น ๆ รวมถึงค่า Previous Hash ของ Block ก่อนหน้านั้นด้วย ทั้งนี้ในการออกแบบโครงสร้าง Block แต่ละแพลตฟอร์มอาจมีการใช้ชื่อเรียกที่แตกต่างกันออกไป



Hash Value

ค่าผลลัพธ์ที่ได้จากกระบวนการทำ Hash Function โดยการนำ Hash Function คือ การนำข้อมูลต้นฉบับที่ต้องการแปลงข้อมูลมาผ่านกระบวนการทางคณิตศาสตร์ ซึ่งเป็นฟังก์ชันทางเดียวในการแปลงข้อมูลให้อยู่ในรูปแบบที่มีลักษณะเฉพาะของข้อมูลและมีขนาดความยาวที่คงที่เสมอโดยข้อมูลต้นฉบับที่ผ่านการทำ Hash Function แล้วจะไม่สามารถดำเนินการย้อนกลับเพื่อให้ได้ซึ่งข้อมูลเดิม

Consensus

การกำหนดข้อตกลงและความเห็นชอบร่วมกันระหว่างสมาชิกในเครือข่าย Blockchain โดยสมาชิกต้องยอมรับกฎระเบียบร่วมกัน ด้วยกลไกในการควบคุมความถูกต้องของข้อมูลในทุก Node ผ่านอัลกอริทึมต่าง ๆ เพื่อให้ข้อมูลมีความถูกต้องเที่ยงตรงและเป็นข้อมูลชุดเดียวกัน รวมทั้งข้อมูลมีการจัดเก็บที่สอดคล้องและมีลำดับการจัดเก็บตรงกัน ทั้งนี้ กระบวนการ Consensus มีอยู่ด้วยกันหลายวิธี โดยการเลือกใช้วิธีใดนั้นขึ้นอยู่กับความเหมาะสมของ Blockchain ในแต่ละประเภท

Proof-of-Work

เป็นกระบวนการ Consensus วิธีหนึ่ง โดยใช้การแก้ปัญหาทางคณิตศาสตร์ซึ่งมีความซับซ้อนและต้องใช้เวลาในการแก้ปัญหาหนึ่ง ๆ จาก Nodes ต่าง ๆ ที่อยู่ในเครือข่ายหรือเรียกว่า “Miner” เพื่อยืนยันความน่าเชื่อถือของข้อมูลที่จะถูกบันทึกเข้ามาในเครือข่าย โดย Miner จะได้รับค่าตอบแทนจากการทำ Proof-of-Work และด้วยวิธีการดังกล่าวทำให้การแก้ไขข้อมูลที่ถูกบันทึกลงในระบบ Blockchain แล้วนั้นทำได้ยากโดยที่ไม่แก้ไขข้อมูลใน Block ถัด ๆ ไป ซึ่งจะต้องทำ Proof-of-Work ในทุก Block ซึ่งค่อนข้างยุ่งยากและใช้เวลาในการคำนวณพอสมควร อีกทั้งยังจะต้องทำการแก้ไขทุก Block ในเวลาเดียวกัน ซึ่งการจะแก้ไขปัญหาดังกล่าวในระยะเวลาที่จำกัดจึงเป็นเรื่องที่เป็นไปได้ยากมากด้วยความสามารถของเครื่องคอมพิวเตอร์ในปัจจุบัน ดังนั้นเป้าหมายการทำ Proof-of-Work ในเทคโนโลยี Blockchain จึงเป็นการป้องกันการโจมตีระบบด้วยการเพิ่มต้นทุนทางเศรษฐศาสตร์ให้กับผู้โจมตี เพื่อให้เกิดความไม่คุ้มค่าที่จะทำการโจมตี

Proof-of-Stake

เป็นกระบวนการ Consensus วิธีหนึ่ง โดยใช้หลักการวาง “สินทรัพย์” ของผู้ตรวจสอบ (Validator) ในการยืนยันธุรกรรม ผู้ตรวจสอบที่ทำการวางสินทรัพย์จำนวนมากจึงมีโอกาสสูงที่จะได้รับสิทธิ์ในการเขียนข้อมูลธุรกรรมบน Block ถัดไป โดยผู้ที่ทำการเขียนข้อมูลบน Block ถัดไปจะได้รับค่าธรรมเนียมการดำเนินงานเป็นรางวัลตอบแทน

Proof-of-Authority

เป็นกระบวนการ Consensus วิธีหนึ่ง โดยทำข้อตกลงร่วมกันในการกำหนดสิทธิ์ผู้ใช้งานหรือองค์กรที่เชื่อถือได้ สำหรับการธุรกรรมด้วยวิธีการระบุชื่อผู้ใช้อย่างเป็นทางการให้กับผู้มีส่วนได้ส่วนเสียแต่ละ Node บนเครือข่าย Blockchain ในการทำธุรกรรมจะได้รับการตรวจสอบสิทธิ์จากบัญชีที่ได้รับอนุมัติหรือเรียกว่า ผู้ตรวจสอบ (Validator) ซึ่งทำหน้าที่ในการรักษาความปลอดภัย โดยใช้รูปแบบการหมุนเวียนสิทธิเพื่อกระจายความรับผิดชอบ และเป็นการสร้างความสัมพันธ์ระหว่างหน่วยงานอย่างเป็นธรรม

Practical Byzantine Fault Tolerance (PBFT)

เป็นกระบวนการ Consensus วิธีหนึ่ง โดยใช้หลักการเสียงข้างมาก ซึ่งต้องมีจำนวนผู้ตรวจสอบ (Validator) ทั้งสิ้นจำนวน $3f+1$ Node เพื่อรับประกันความถูกต้องของระบบ โดย f คือ จำนวนผู้ตรวจสอบที่ไม่สามารถทำงานได้ในขณะนั้น

Public Blockchain/ Permissionless Blockchain

Blockchain วงเปิดที่อนุญาตให้ทุกคนสามารถเข้าใช้งาน ไม่ว่าจะเป็นการอ่าน หรือการทำธุรกรรมต่าง ๆ ได้อย่างอิสระ โดยไม่จำเป็นต้องขออนุญาต ตัวอย่างของระบบ Blockchain แบบเปิดสาธารณะ เช่น Bitcoin, Ethereum

Private Blockchain/ Permission Blockchain

Blockchain วงปิดที่เข้าใช้งานได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น ซึ่งส่วนใหญ่เป็นการสร้างขึ้นเพื่อใช้งานภายในองค์กร ดังนั้นข้อมูลการทำธุรกรรมต่าง ๆ จะถูกจำกัดอยู่เฉพาะภายในเครือข่าย ซึ่งประกอบไปด้วยสมาชิกที่ได้รับอนุญาตเท่านั้น ตัวอย่างของระบบ Blockchain แบบปิด เช่น Hyperledger, Corda, Tendermint

Consortium Blockchain

Blockchain ที่เปิดให้ใช้งานได้เฉพาะกลุ่มเท่านั้น ซึ่งส่วนมากจะเป็นการรวมตัวกันขององค์กรที่มีลักษณะธุรกิจเหมือนกัน และต้องมีการแลกเปลี่ยนข้อมูลระหว่างกัน ยกตัวอย่างเช่น เครือข่ายระหว่างธนาคาร ที่ใช้ในการแลกเปลี่ยนข้อมูลการทำธุรกรรม หรือแลกเปลี่ยนสินทรัพย์ภายในกลุ่มของธนาคาร เช่น Japanese Bank และ R3CEV

Merkle Root

ค่า Hash ที่อยู่บนสุดของ Hash Tree โดยค่าดังกล่าวจะถูกแสดงใน Block Information ซึ่ง Hash Tree จะใช้กับการออกแบบ Block ที่มีการรวบรวม Transaction ที่เกิดขึ้นในเวลาไล่เลี่ยกัน รวมเข้าไว้ใน Block เดียวกัน โดยทำการ Hash รายการ Transaction ทั้งหมดใน Block ซึ่งเป็นวิธีการ Hash ข้อมูลชุดใหญ่ โดยใช้รูปแบบ Hash Tree ซึ่งจะ Hash Transactions ทั้งหมดใน Block ให้กลายเป็น Hash Value ขนาด 32 ไบต์

Ethereum

เป็น Platform ของ Blockchain แบบเปิด (Public Blockchain) โดย Ethereum มีความแตกต่างจาก Bitcoin เนื่องจาก Ethereum ถูกออกแบบมาเพื่อให้สามารถปรับตัวได้และมีความยืดหยุ่น อีกทั้งยังเป็น Open Source โดยความสามารถของ Ethereum ถือว่าทัดเทียมกับ Bitcoin แต่สิ่งที่เพิ่มขึ้นมา คือ ฟังก์ชันที่เรียกว่า Smart Contract ที่อนุญาตให้ผู้ใช้งาน หรือนักพัฒนาโปรแกรม สามารถเขียนโปรแกรมลงในข้อมูลของสกุลเงิน Ether ได้ เพื่อให้ทำงานอัตโนมัติเมื่อเงื่อนไขเป็นไปตามที่กำหนด ในสัญญา ดังนั้นจึงทำให้สามารถสร้าง Application ต่าง ๆ ขึ้นมาบนเครือข่าย Ethereum อีกชั้นหนึ่งได้ ทำให้เกิดรูปแบบที่หลากหลายในการใช้งานซึ่งแตกต่างจาก Bitcoin ที่เน้นการทำธุรกรรมเพียงอย่างเดียว

Cryptocurrency

สกุลเงินดิจิทัลซึ่งมีมูลค่าเหมือนกับธนบัตรในสกุลเงินประเทศต่าง ๆ และถูกใช้เป็นตัวกลางในการแลกเปลี่ยนแบบดิจิทัล โดยการแลกเปลี่ยนรูปแบบดิจิทัลได้เริ่มขึ้นเมื่อปี ค.ศ. 2009 ซึ่ง Blockchain Application ในกลุ่มเงินดิจิทัลได้ถูกพัฒนาขึ้นเพื่อใช้ในธุรกิจการให้บริการทางการเงินทั้งการโอนและการจ่ายเงิน ยกตัวอย่างเช่น Bitcoin และ Ripple

Ledger

บัญชีประวัติการทำธุรกรรมซึ่งจะถูกบันทึกและทำสำเนา แจกจ่ายให้กับทุก Node ที่อยู่ในเครือข่าย Blockchain

Oracle

แหล่งข้อมูลที่เชื่อถือได้จากภายนอกในระบบ Blockchain (Trusted 3rd Party Source) ซึ่ง Smart Contract จะนำมาอ้างอิงเพื่อบังคับใช้ สัญญาตามที่เขียนโปรแกรมไว้ เช่น แหล่งข้อมูลระดับน้ำ ของแต่ละพื้นที่เพื่อให้ค่าธรรมเนียมประกันอุทกภัยที่เขียนด้วย Smart Contract ใช้สำหรับอ้างอิงการเคลมประกันแบบอัตโนมัติ

Smart Contract

สัญญาอัจฉริยะโดยจะเก็บเงื่อนไขหรือข้อตกลงของสัญญาต่าง ๆ ไว้ในรูปแบบ Code คอมพิวเตอร์ ซึ่งจะถูกเก็บไว้ในเครือข่าย Blockchain

Node

อุปกรณ์ในเครือข่าย Blockchain เปรียบได้กับเครื่อง คอมพิวเตอร์ โทรศัพท์ หรืออื่น ๆ ที่สามารถเชื่อมต่อ อินเทอร์เน็ตและประมวลผลได้ ซึ่งถือว่าเป็นโครงสร้างพื้นฐาน ที่สำคัญในการกระจายและเชื่อมโยงกันในเครือข่ายเพื่อให้ ระบบสามารถทำงานและประมวลผลได้ ทั้งนี้ประเภทของ Node ในเครือข่าย Blockchain สามารถจำแนกได้เป็น

1. Node ที่ทำหน้าที่ในการจัดเก็บสำเนาข้อมูลเท่านั้น ประกอบด้วย Full Node และ Light Node
2. Node ที่ทำหน้าที่ตรวจสอบความถูกต้องเท่านั้น หรือที่รู้จักกันในชื่อ Consensus Node

A group of business professionals in a meeting, overlaid on a city skyline at night. The image has a blue color cast and a grid pattern. The text '01' is prominently displayed in the center.

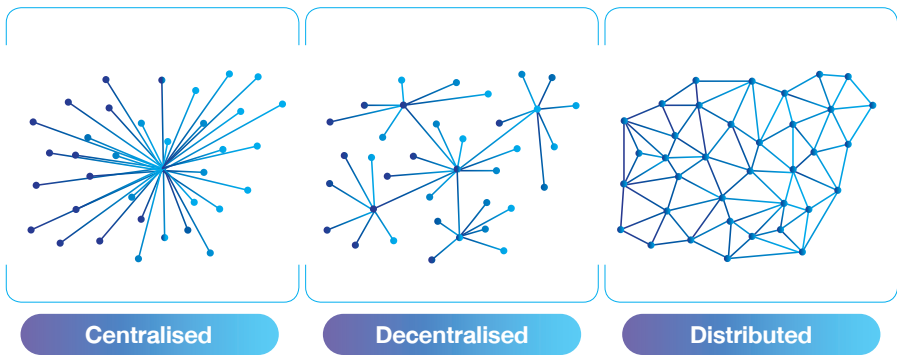
01

บทนำ

เทคโนโลยี Blockchain

Blockchain คือเทคโนโลยีการจัดเก็บข้อมูลแบบ Shared Database หรือที่รู้จักกันในชื่อ “Distributed Ledger Technology (DLT)” โดยเป็นรูปแบบการบันทึกข้อมูลที่รับประกันความปลอดภัยว่าข้อมูลที่ถูกบันทึกไปก่อนหน้านี้ไม่สามารถที่จะเปลี่ยนแปลง หรือแก้ไขได้ ซึ่งทุกผู้ใช้งานจะได้เห็นข้อมูลชุดเดียวกันทั้งหมด โดยใช้หลักการ Cryptography และความสามารถของ Distributed Computing เพื่อสร้างกลไกความน่าเชื่อถือ (Yermack, 2017)

จุดเริ่มต้นของเทคโนโลยี Blockchain เกิดขึ้นครั้งแรกในปี 2008 โดยการนำเสนอของ “Satoshi Nakamoto” จากเอกสาร Bitcoin: A Peer-to-Peer Electronic Cash System เป็นการนำเสนอแนวคิดเกี่ยวกับการสร้าง Platform ที่สามารถสร้างความปลอดภัยในการแลกเปลี่ยนเงินสกุลดิจิทัลที่มีชื่อว่า “Bitcoin” โดยใช้ทฤษฎีเกี่ยวกับการทำ Cryptography และ Distributed Computing ดังแสดงในรูปภาพที่ 1



รูปภาพที่ 1: s:UUUU Centralised, Decentralised IIa: Distributed

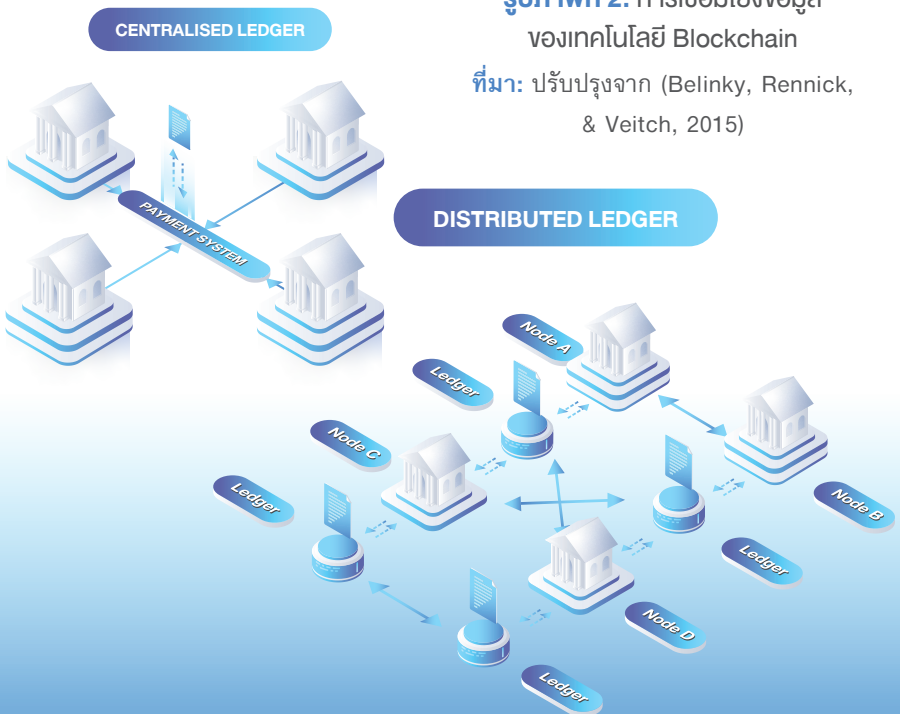
ที่มา: ปรับปรุงจาก (Baran, 1964)

ซึ่งไม่จำเป็นต้องมีคนกลางเข้ามาเกี่ยวข้อง เช่น ธนาคาร หรือหน่วยงานอื่น ๆ ที่เกี่ยวข้องกับการโอนเงิน โดยได้รับความสนใจอย่างแพร่หลาย รวมทั้งได้รับการยอมรับจากผู้เชี่ยวชาญทั่วโลกว่าเป็นเทคโนโลยีที่มีศักยภาพ และสามารถนำมาประยุกต์ใช้ในภาคธุรกิจอื่น ๆ ได้ไม่จำเพาะแค่ภาคธุรกิจการเงินและการธนาคารเท่านั้น แต่ยังรวมถึงภาครัฐก็ได้มีการตื่นตัวและศึกษาเกี่ยวกับเทคโนโลยี Blockchain กันอย่างแพร่หลายเช่นกัน

การทำงานของเทคโนโลยี Blockchain อาศัยการจัดเก็บข้อมูลแบบกระจายศูนย์ (Distributed Ledger Technology) โดยทุกข้อมูลจะมีการเชื่อมโยงกันทั้งระบบ และเมื่อมีรายการธุรกรรมใหม่เกิดขึ้นจะต้องมีการประกาศบอกทุกเครื่องในระบบให้รับรู้ ดังแสดงในรูปภาพที่ 2

รูปภาพที่ 2: การเชื่อมโยงข้อมูลของเทคโนโลยี Blockchain

ที่มา: ปรับปรุงจาก (Belinky, Rennick, & Veitch, 2015)





PROTECT YOUR DATA

นอกจากนี้รายการธุรกรรมดังกล่าวจะต้องผ่านการตรวจสอบ (Consensus) จากทั้งเครือข่ายเสียก่อน จึงจะสามารถบันทึกข้อมูลเข้า Block ได้ ดังนั้นเทคโนโลยี Blockchain จึงไม่จำเป็นต้องมีตัวกลางคอยทำหน้าที่ในการจัดเก็บรายการธุรกรรม แต่ข้อมูลทั้งหมดจะถูกจัดเก็บอยู่ภายใต้โครงสร้างของเทคโนโลยี Blockchain และถูกกระจายไปยังเครื่องของสมาชิกทุกคนในเครือข่าย และถ้ามีคนพยายามสร้างรายการธุรกรรมปลอมขึ้นมา ข้อมูลก็จะขัดแย้งกับข้อมูลในเครื่องของสมาชิกอื่น ๆ ในเครือข่าย เนื่องจากทุกเครื่องจะต้องมีข้อมูลเหมือนกันทั้งหมด ดังนั้นระบบจะไม่อนุญาตให้สร้างรายการดังกล่าว โดยจะมีแต่รายการที่ทุกคนในเครือข่ายยอมรับเท่านั้นที่จะสามารถบันทึกเข้าสู่ระบบ Blockchain ได้ และข้อมูลที่ถูกบันทึกเข้าสู่ระบบ Blockchain ไปแล้วจะไม่สามารถเปลี่ยนแปลงหรือแก้ไขย้อนหลังได้ จึงทำให้เทคโนโลยี Blockchain ได้รับการยอมรับว่าเป็นเทคโนโลยีการจัดเก็บข้อมูลที่มีความน่าเชื่อถือสูง

หลักการงานของเทคโนโลยี Blockchain

หลักการงานของเทคโนโลยี Blockchain คือ ฐานข้อมูลจะถูกแชร์ให้กับทุก Node¹ ที่อยู่โนเครือข่ายและการทำงานของเทคโนโลยี Blockchain จะไม่มีเครื่องใดเครื่องหนึ่งเป็นศูนย์กลางหรือเครื่องแม่ข่าย ซึ่งการทำงานแบบกระจายศูนย์นี้จะไม่ถูกควบคุมโดยคนเพียงคนเดียว แต่ทุก Node จะได้รับสำเนาฐานข้อมูลเก็บไว้และจะมีการอัปเดตฐานข้อมูลแบบอัตโนมัติเมื่อมีข้อมูลใหม่เกิดขึ้น ทั้งนี้สำเนาฐานข้อมูลของทุกคนในเครือข่ายจะต้องถูกต้อง และตรงกันกับของสมาชิกคนอื่นในเครือข่าย อีกทั้งการบันทึกข้อมูลเข้าสู่ Block ยังอาศัยหลักการทำ Cryptography และการทำ Consensus² จากสมาชิกในเครือข่ายด้วยกันก่อนทำการบรรจุข้อมูลลง

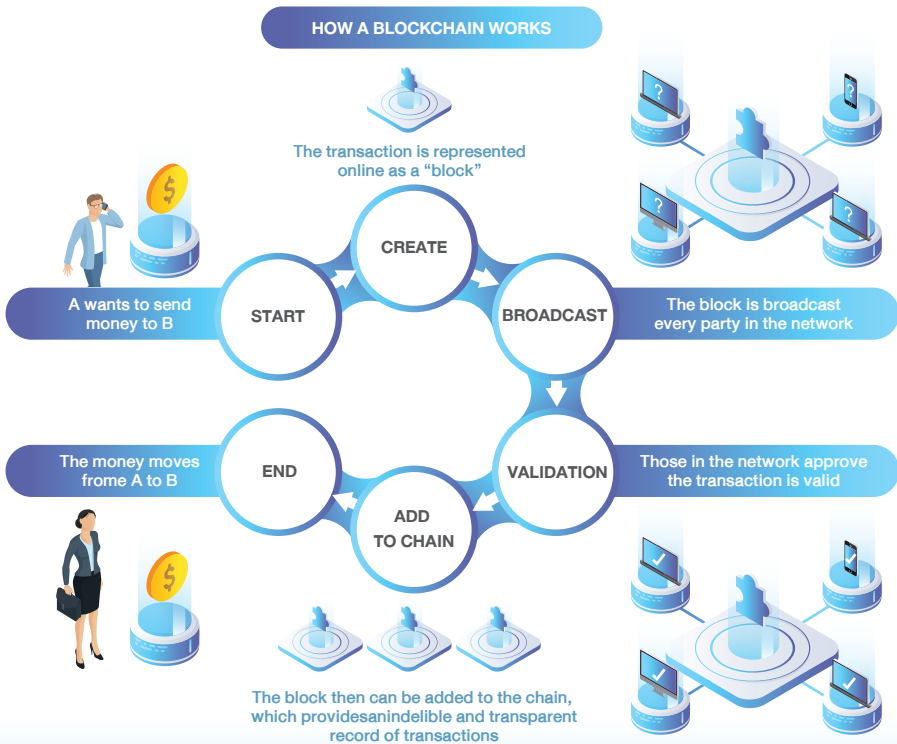
¹ Node คือ อุปกรณ์ในเครือข่าย Blockchain เปรียบได้กับเครื่องคอมพิวเตอร์ โทรศัพท์ หรืออื่น ๆ ที่สามารถเชื่อมต่ออินเทอร์เน็ตและประมวลผลได้ ซึ่งถือว่าเป็นโครงสร้างพื้นฐานที่สำคัญในการกระจายและเชื่อมโยงกันเครือข่ายเพื่อให้ระบบสามารถทำงานและประมวลผลได้ ทั้งนี้ประเภทของ Node ในเครือข่าย Blockchain สามารถจำแนกได้เป็น

1) Node ที่ทำหน้าที่ในการจัดเก็บสำเนาข้อมูลเท่านั้น ประกอบด้วย Full Node และ Light Node

2) Node ที่ทำหน้าที่ตรวจสอบความถูกต้องเท่านั้น หรือที่รู้จักกันในชื่อ Consensus Node

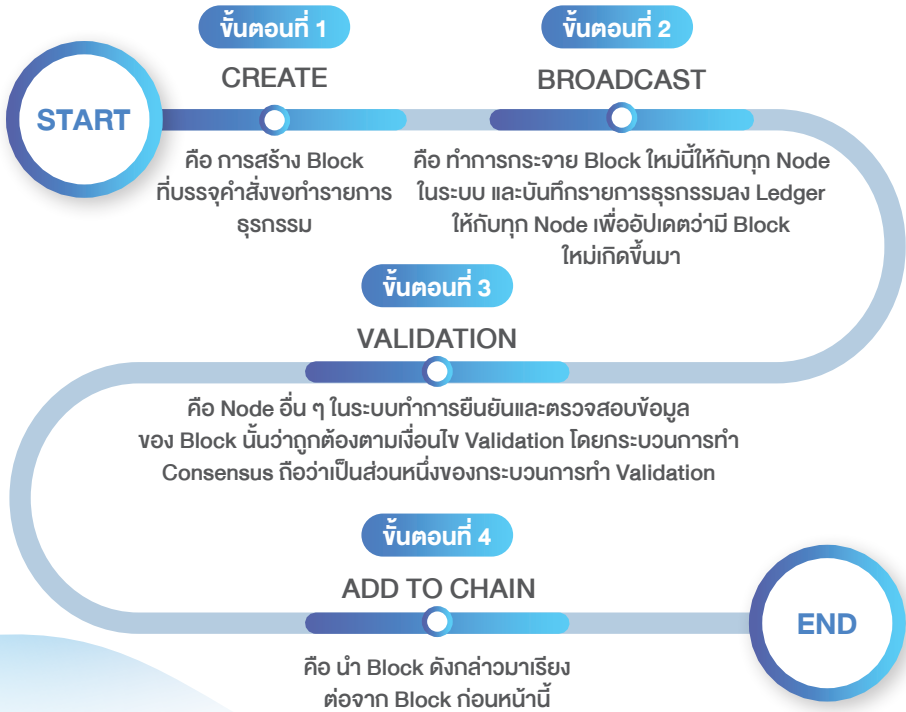
² Consensus คือ การกำหนดข้อตกลงและความเห็นชอบร่วมกันระหว่างสมาชิกในเครือข่าย Blockchain โดยสมาชิกต้องยอมรับกฎระเบียบร่วมกัน ด้วยกลไกในการควบคุมความถูกต้องของข้อมูลในทุก Node ผ่านอัลกอริทึมต่าง ๆ เพื่อให้ข้อมูลมีความถูกต้องเที่ยงตรงและเป็นข้อมูลชุดเดียวกัน รวมทั้งข้อมูลมีการจัดเก็บที่สอดคล้องและมีลำดับการจัดเก็บตรงกัน ทั้งนี้กระบวนการ Consensus มีอยู่ด้วยกันหลายวิธี โดยการเลือกใช้วิธีใดนั้น ขึ้นอยู่กับความเหมาะสมของ Blockchain ในแต่ละประเภท

Block และเพิ่มเข้าสู่ระบบ Blockchain เพื่อเป็นการป้องกัน และรับประกันความปลอดภัยของข้อมูล โดยแต่ละเครือข่าย Blockchain จะมีการกำหนดกฎเกณฑ์ในการตรวจสอบหรือที่เรียกว่า “Consensus Protocol” หรือ “Consensus Mechanism” ขึ้นมาเพื่อใช้ในเครือข่าย โดยหลักการทำงานพื้นฐานที่สำคัญของเทคโนโลยี Blockchain อย่างน้อยจะต้องประกอบไปด้วย 4 ขั้นตอนหลัก ๆ ดังแสดงในรูปภาพที่ 3



รูปภาพที่ 3: หลักการทำงานของเทคโนโลยี Blockchain

ที่มา: ปรับปรุงจาก (Veedvil, 2017)



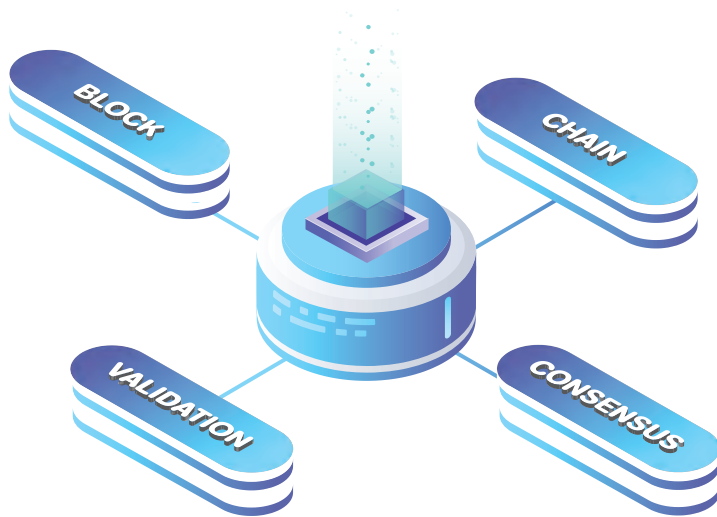
อย่างไรก็ดี ในการออกแบบการทำงานของระบบ Blockchain ในการทำงานจริง อาจจะมีการออกแบบขั้นตอนการทำงานที่แตกต่างไปจากนี้ได้ ขึ้นอยู่กับการออกแบบของแต่ละผู้ผลิต หรือแต่ละ Platform แต่อย่างน้อยจะต้องมี 4 ขั้นตอนหลักนี้ซึ่งถือได้ว่าเป็นหัวใจสำคัญของการทำงาน Blockchain นั้นเอง



องค์ประกอบของเทคโนโลยี Blockchain

องค์ประกอบของเทคโนโลยี Blockchain ประกอบด้วย 4 องค์ประกอบสำคัญ คือ

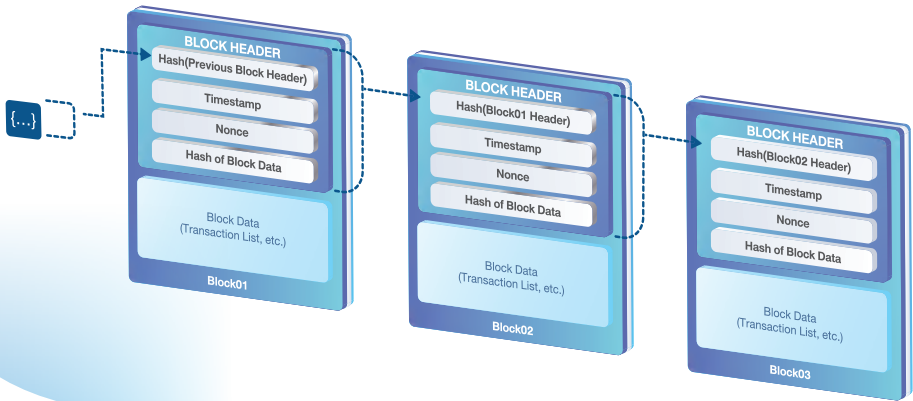
1) Block 2) Chain 3) Consensus และ 4) Validation ดังแสดงในรูปภาพที่ 4



รูปภาพที่ 4: องค์ประกอบของเทคโนโลยี Blockchain

ที่มา: ปรับปรุงจาก (Veedvil, 2017)

การจัดเก็บข้อมูลของเทคโนโลยี Blockchain จะถูกจัดเก็บในรูปแบบของ Block โดยแต่ละ Block จะเชื่อมโยงเข้าหา Block ก่อนหน้าด้วยค่า Hash Function ของ Block ก่อนหน้านี้เสมอ และจะเรียงร้อยต่อกันเป็น Chain ทำให้ยากต่อการปลอมแปลงแก้ไข และสามารถตรวจสอบความถูกต้องของข้อมูลได้ทุก ๆ Block ตลอดทั้ง Chain ซึ่งสามารถตรวจสอบย้อนกลับไปได้จนถึง Block เริ่มต้น หรือ Genesis Block ได้ (Yaga, Mell, Roby, & Scarfone, 2018) ดังแสดงในรูปภาพที่ 5

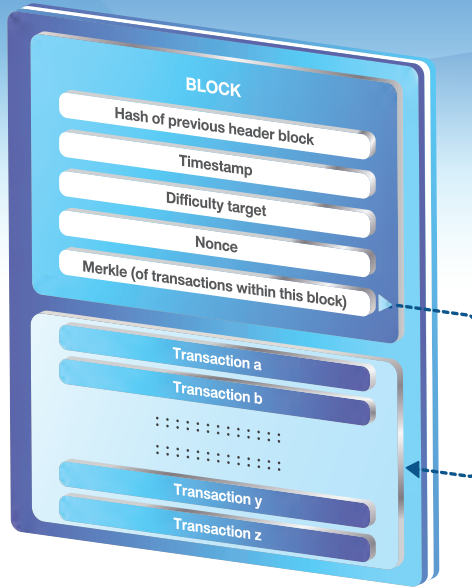


รูปภาพที่ 5: โครงสร้างการเชื่อมโยง Block

ที่มา: ปรับปรุงจาก (Yaga, Mell, Roby, & Scarfone, 2018b)

ดังนั้น Block คือ ชุดบรรจุข้อมูล แบ่งออกเป็น 2 ส่วน คือ ส่วนของ Block Header เพื่อใช้บอกให้คนอื่นทราบว่าภายในบรรจุข้อมูลอะไรไว้ และส่วนของ Block Data เพื่อใช้ในการบรรจุข้อมูลต่าง ๆ ยกตัวอย่างเช่น ข้อมูลจำนวนเงิน ข้อมูลการโอนเงิน ข้อมูลประวัติการรักษาพยาบาล หรือข้อมูลอื่น ๆ โดยโครงสร้างของแต่ละ Block จะประกอบไปด้วยข้อมูล 7 ส่วน ดังแสดงในรูปภาพที่ 6





รูปภาพที่ 6: โครงสร้างภายใน Block ของ Bitcoin
ที่มา: ปรับปรุงจาก (Nakamoto, 2008)

- 1 **หมายเลข Block** คือ ตัวเลขจำนวนเต็มเรียงกันตั้งแต่ 1, 2, 3, 4, 5 ไปเรื่อย ๆ โดยมีความหมายแสดงถึงลำดับก่อนหลัง คือ Block หมายเลข 1 เกิดขึ้นก่อน Block หมายเลข 2 และ Block หมายเลข 1 อยู่ติดกับหมายเลข 2 เป็นต้น
- 2 **Timestamp** คือ เวลาที่ Block นั้น ๆ ถูกสร้างขึ้นมา
- 3 **Nonce** คือ ค่าที่ใช้ในการค้นหาค่า Hash ของ Block ตามกฎของระบบที่ได้กำหนดไว้ ซึ่งกฎดังกล่าวคือ Proof-of-Work หมายความว่า หากเราต้องการจะสร้าง Block ขึ้นมาสัก Block หนึ่งในระบบ Blockchain เราจะต้องแสดงให้เห็นว่า เราได้ทำการแก้ปัญหาหรือทำงาน (Work) ตามกฎที่กำหนดไว้แล้ว

4 **Difficulty Target** คือ ค่าระดับความยากที่จะถูกใช้ในการค้นหาค่า Nonce โดยค่า Hash ที่ได้นั้นจะต้องมีค่าต่ำกว่าค่า Difficulty Target นั้นเอง

5 **Previous Hash** คือ ค่า Current Hash ของ Block ก่อนหน้า ซึ่งเปรียบได้กับค่า Digital Signature ของ Block ก่อนหน้าโดยจะถูกจัดเก็บอยู่ในโครงสร้างของ Block ถัดไปเสมอ และหากมีการแก้ไขข้อมูลใน Block ก่อนหน้าจะทำให้ค่า Hash ของ Block ไม่เท่ากัน ทั้งนี้ในการออกแบบโครงสร้าง Block แต่ละแพลตฟอร์มอาจมีการใช้ชื่อเรียกที่แตกต่างกันออกไป

6 **Data** คือ ข้อมูลที่ถูกบันทึกอยู่ใน Block ซึ่งข้อมูลนี้จะเป็นอะไรก็ได้ที่เราจะบันทึก เช่น ข้อมูล Transaction ต่าง ๆ เป็นต้น

7 **Merkle Root** คือ ค่า Hash ของ Transactions ทั้งหมดใน Block ซึ่งเป็นวิธีการ Hash ข้อมูลชุดใหญ่ โดยใช้รูปแบบ Hash Tree ซึ่งจะ Hash Transactions ทั้งหมดใน Block ให้กลายเป็น Hash Value³ ขนาด 32 ไบต์

³ Hash Value คือ ค่าผลลัพธ์ที่ได้จากกระบวนการทำ Hash Function โดยการนำข้อมูลต้นฉบับที่ต้องการแปลงข้อมูลมาผ่านกระบวนการทางคณิตศาสตร์ ซึ่งเป็นฟังก์ชันทางเดียวในการแปลงข้อมูลให้อยู่ในรูปแบบที่มีลักษณะเฉพาะของข้อมูลและมีขนาดความยาวที่คงที่เสมอโดยข้อมูลต้นฉบับที่ผ่านการทำ Hash Function แล้วจะไม่สามารถดำเนินการย้อนกลับเพื่อให้ได้ซึ่งข้อมูลเดิม



วิธีการคำนวณค่า Nonce

Nonce คือ ค่าที่ใช้ในการค้นหาค่า Hash ของ Block ซึ่งจะต้องเป็นไปตามกฎของระบบที่ได้กำหนดไว้ โดยค่า Hash ที่ได้นั้นจะต้องมีค่าต่ำกว่าค่า Target หรืออีกชื่อหนึ่ง คือ ค่า Difficulty นั้นเอง โดยคำสั่งดังกล่าวก็คือ “จงทำให้ Hash ของ Block_Header มีค่า \leq Target” โดยค่า Nonce จะถูกวางไว้ใน Block Header ดังแสดงในรูปภาพที่ 7 เพื่อให้เราวนค่าไปเรื่อย ๆ จนกว่าค่า Hash จะต่ำกว่าค่า Target ดังนั้นการหาค่า Nonce ก็คือ การเปลี่ยนค่า Block Header จนกระทั่งได้ค่า Hash ที่ต่ำกว่าค่า Target ให้ได้ ใครหาได้ก่อนคนนั้นชนะซึ่งก็คือ คนที่ได้เป็นคนยืนยันความถูกต้องของ Block นั้น ๆ นั้นเอง ดังนั้นเมื่อได้ค่า Nonce แล้วค่า Hash ที่ได้จากการหาค่า Nonce นั้นก็จะถูกใช้เป็นค่า Hash ของ Block นั้นทันที ซึ่งก็คือ Current Hash ของ Block นั้น ๆ นั้นเอง

ตัวอย่างการแสดงผล BLOCK INFORMATION ของ BITCOIN

```
{
  "ver": 2,
  "prev_block": "0000000000001164214d7b57f6db15b6a354146edc700bef115888ddf558e4",
  "merkle_root": "d2d9daef3bd359ad07b528f856b2115056406e312f912ec4ecde04b3fba7cdf4",
  "time": 1364758683,
  "bits": 436371822,
  "nonce": 2131806299,
  ...
}
```

รูปภาพที่ 7: ตัวอย่างการแสดงผล Block Information ของ Bitcoin

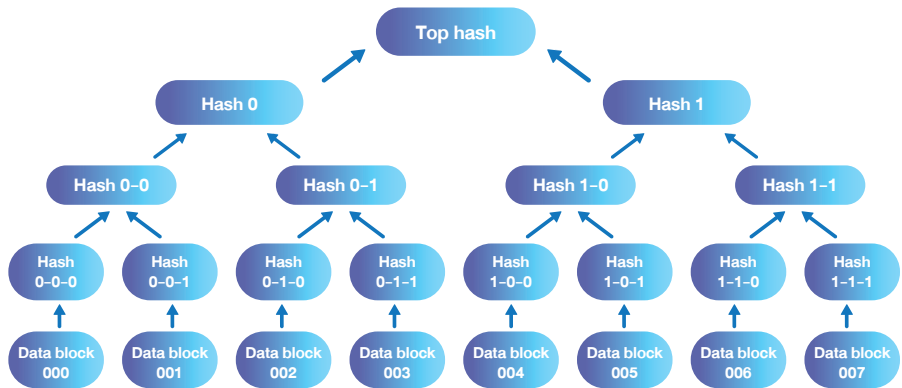
ที่มา: ปรับปรุงจาก (Nuuneoi, 2016)

ค่า Target หรือ Difficulty จะถูกกำหนดโดยระบบภายใต้สูตร

$$\text{Difficulty} = \frac{0x00ffff00}{\text{CurrentTarget}}$$

นอกจากนี้ค่า Target หรือ Difficulty จะถูกคำนวณค่าใหม่ในทุก 2016 Blocks (ประมาณ 2 สัปดาห์) และถูกคำนวณตรง ๆ เลย ถ้า 2016 Blocks ที่ผ่านมาใช้เวลานาน 2 สัปดาห์ ก็จะลดค่า Difficulty ลง แต่ถ้าใช้เวลาน้อยกว่า 2 สัปดาห์ ก็จะปรับค่า Difficulty ขึ้น

จากตัวอย่างการแสดงผล Block Information ในรูปภาพที่ 7 ซึ่งเป็นตัวอย่าง Block Information ของ Bitcoin จะเห็นค่า Merkle Root ซึ่งก็คือ ค่า Hash ของ Transactions ทั้งหมดใน Block ซึ่งเป็นวิธีการ Hash ข้อมูลชุดใหญ่ โดยใช้รูปแบบ Hash Tree ซึ่งจะ Hash Transactions ทั้งหมดใน Block ให้กลายเป็น Hash Value ขนาด 32 ไบต์ ดังแสดงในรูปภาพที่ 8



รูปภาพที่ 8: หลักการ Hash ข้อมูลชุดใหญ่โดยใช้รูปแบบ Hash Tree

ที่มา: ปรับปรุงจาก (Futter, Hale, Elverston, & Waters, 2017)



ดังนั้นค่า Merkle Root ก็คือ ค่า Hash ที่อยู่บนสุดของ Hash Tree นั้นเอง โดยค่าดังกล่าวจะถูกแสดงใน Block Information ซึ่ง Hash Tree จะใช้กับการออกแบบ Block ที่มีการรวม Transaction ที่เกิดขึ้นในเวลาใกล้เคียงกันรวมเข้าไว้ใน Block เดียวกัน



เนื่องจากการกำหนดให้ทุก ๆ Node จะต้องทำการแก้ปัญหาทางคณิตศาสตร์ (A Mathematical Puzzle) หรือที่รู้จักกันในชื่อ "Proof-of-Work" โดย Block ที่ถูกยอมรับจะต้องมีคำตอบของการแก้ปัญหาทางคณิตศาสตร์ดังกล่าวรวมอยู่ใน Block ด้วยซึ่งก็คือการหาค่า Nonce นั้นเอง ดังนั้นจึงเป็นไปได้ที่ผู้โจมตีจะสร้าง Transaction ปลอมขึ้นมาโดยที่ไม่ทำการแก้ไขปัญหาทางคณิตศาสตร์ของ Block นั้น ๆ รวมไปถึง Block อื่น ๆ ที่อยู่ใน Chain ด้วย อีกทั้งจะต้องทำพร้อม ๆ กันในทุก ๆ Block เพื่อให้ได้รับการยอมรับจาก Node อื่น ๆ ซึ่งเป็นสิ่งที่ยากและแทบจะเป็นไปไม่ได้เลยด้วยความสามารถของเครื่องคอมพิวเตอร์ที่มีอยู่ในปัจจุบัน จึงทำให้ Blockchain ได้รับการยอมรับว่าเป็นรูปแบบของการบันทึกข้อมูลที่มีความปลอดภัยสูง



Chain

Chain คือ หลักการจดจำทุก ๆ อุดมกรรมของทุก ๆ คนในระบบและบันทึกข้อมูลพร้อมจัดทำเป็นสำเนาบัญชี Ledger แจกจ่ายให้กับทุกคนในระบบ สำเนาบัญชี Ledger ที่ว่านั้นจะถูกกระจายส่งต่อไปให้ทุก ๆ Node ในระบบเพื่อให้ทุกคนรับทราบว่ามีธุรกรรมอะไรเกิดขึ้นมาบ้างตั้งแต่เปิดระบบ Blockchain นั้นขึ้นมา ถึงแม้ว่าจะมี Node ใด Node หนึ่งเสียหายไปก็สามารถยืนยันหรือกู้ข้อมูล Ledger จาก Node อื่น ๆ กลับมาอัปเดตให้ทั้งระบบได้เหมือนเดิม



Consensus

การกำหนดข้อตกลงและความเห็นชอบร่วมกันระหว่างสมาชิกในเครือข่าย Blockchain โดยสมาชิกต้องยอมรับกฎระเบียบร่วมกัน ด้วยกลไกในการควบคุมความถูกต้องของข้อมูลในทุก Node ผ่านอัลกอริทึมต่าง ๆ เพื่อให้ข้อมูลมีความถูกต้องเที่ยงตรงและเป็นข้อมูลชุดเดียวกัน รวมทั้งข้อมูลมีการจัดเก็บที่สอดคล้องและมีลำดับการจัดเก็บตรงกัน ทั้งนี้ กระบวนการ Consensus มีอยู่ด้วยกันหลายวิธี ยกตัวอย่างเช่น



Proof-of-Work คือ กระบวนการทำ Consensus โดยการใช้การแก้ปัญหาทางคณิตศาสตร์ซึ่งมีความซับซ้อนและต้องใช้เวลาในการแก้ปัญหานั้น ๆ จาก Nodes ต่าง ๆ ที่อยู่ในเครือข่ายหรือเรียกว่า “Miners” เพื่อยืนยันความน่าเชื่อถือของข้อมูลที่จะถูกบันทึกเข้ามาในเครือข่าย โดย Miner จะได้รับค่าตอบแทนจากการทำ Proof-of-Work และด้วยวิธีการดังกล่าวทำให้การแก้ไขข้อมูลที่ถูกบันทึกลงในระบบ Blockchain แล้วนั้นทำได้ยากโดยที่ไม่แก้ไขข้อมูลใน Block ถัด ๆ ไป ยกตัวอย่างเช่น Bitcoins ซึ่งเป็น Public Blockchain ใช้วิธีการยืนยันรายการแบบ Proof-of-Work



Proof-of-Stake คือ กระบวนการทำ Consensus โดยใช้หลักการวาง “สินทรัพย์” ของผู้ตรวจสอบ (Validator) ในการยืนยันธุรกรรม ผู้ตรวจสอบที่ทำการวางสินทรัพย์จำนวนมากจึงมีโอกาสสูงที่จะได้รับสิทธิ์ในการเขียนข้อมูลธุรกรรมบน Block ถัดไป โดยผู้ที่ทำการเขียนข้อมูลบน Block ถัดไปจะได้รับค่าธรรมเนียมการดำเนินงานเป็นรางวัลตอบแทน ยกตัวอย่างเช่น Ethereum ซึ่งเป็น Public Blockchain ใช้วิธีการยืนยันรายการแบบ Proof-of-Stake



Practical Byzantine Fault Tolerance (PBFT) คือ กระบวนการทำ Consensus โดยใช้หลักการเสียงข้างมาก ซึ่งต้องมีจำนวนผู้ตรวจสอบ (Validator) ทั้งสิ้นจำนวน $3f+1$ node เพื่อรับประกันความถูกต้องของระบบ โดย f คือ จำนวนผู้ตรวจสอบที่ไม่สามารถทำงานได้ในขณะนั้น ยกตัวอย่างเช่น HyperLedger ซึ่งเป็น Private Blockchain ใช้วิธีการยืนยันรายการแบบ PBFT



Proof-of-Authority คือ กระบวนการ Consensus โดยใช้การทำข้อตกลงร่วมกันในการกำหนดสิทธิผู้ใช้งานหรือองค์กรที่เชื่อถือได้ สำหรับการทำธุรกรรมด้วยวิธีการระบุชื่อผู้ใช้อย่างเป็นทางการให้กับผู้มีส่วนได้ส่วนเสียแต่ละ Node บนเครือข่าย Blockchain ในการทำธุรกรรมจะได้รับการตรวจสอบสิทธิ์จากบัญชีที่ได้รับอนุมัติหรือเรียกว่าผู้ตรวจสอบ (Validator) ซึ่งทำหน้าที่ในการรักษาความปลอดภัย โดยใช้รูปแบบการหมุนเวียนสิทธิเพื่อกระจายความรับผิดชอบ และเป็นการสร้างความสัมพันธ์ระหว่างหน่วยงานอย่างเป็นทางการ

จากตัวอย่างที่ได้กล่าวมาข้างต้นนั้นเป็น Consensus Mechanisms ที่ได้รับการยอมรับและถูกนำไปใช้ในเครือข่าย Blockchain ที่มีชื่อเสียงหลาย ๆ เครือข่ายด้วยกัน แต่วิธีการดังกล่าวก็เป็นเพียงส่วนหนึ่งของ Consensus Mechanisms เท่านั้น ซึ่งในการใช้งานจริงยังมีอีกหลายวิธี เช่น Ledger Based, Proprietary Distributed Ledger Consensus, Federated Consensus, N2N, Delegated Proof of Stake และ Round Robin โดยการเลือกใช้วิธีใดนั้นขึ้นอยู่กับความเหมาะสมของ Blockchain ในแต่ละประเภท รวมถึงแนวทางการออกแบบระบบ Blockchain





Validation

Validation คือ การตรวจสอบความถูกต้องแบบทบทวนทั้งระบบและทุก Node ในระบบ Blockchain เพื่อให้แน่ใจว่าจะไม่มีข้อผิดพลาดเกิดขึ้นไม่ว่าจะมาจากส่วนใดก็ตาม ซึ่งก็คือส่วนหนึ่งของ Consensus ที่เรียกว่า Proof-of-Work ซึ่งในหลักการแล้วการทำ Validation นั้นมีจุดประสงค์อยู่ 3 ประการคือ

1 วิธีการในการยอมรับ/ปฏิเสธ รายการใน Block นั้น ๆ

2 วิธีการตรวจสอบที่ทุกคนในระบบยอมรับร่วมกัน

3 วิธีตรวจสอบความถูกต้องของแต่ละ Block ยกตัวอย่างเช่น



หมายเลข Block โดยตรวจสอบ Block ก่อนหน้าที่ติดกันก่อนว่าเป็น Block ที่ถูกต้องหรือไม่โดยเวลาที่ Block ถูกสร้างขึ้นต้องมากกว่าเวลาของ Block ก่อนหน้า



ค่า Nonce โดยการตรวจสอบค่า Nonce ซึ่งก็คือค่า Hash ของ Block ที่ได้มาจากการทำ Proof-of-Work นั้นเอง



ค่า Previous Hash และ ค่า Current Hash โดยการตรวจสอบสถานะเริ่มต้นใน Block ต้องมีข้อมูลตรงตามสถานะสุดท้ายของ Block ก่อนหน้า

แต่อย่างไรก็ดีวิธีการตรวจสอบความถูกต้องของแต่ละ Block หรือการทำ Validation นั้นอาจจะมีขั้นตอนมากกว่านี้ขึ้นอยู่กับกระบวนการเก็บข้อมูลใน Block ของแต่ละค่ายนั่นเอง ยกตัวอย่างเช่น ค่าย Ethereum นั้นจะมีขั้นตอนการ Validation ถึง 5 ขั้นตอนด้วยกัน ซึ่งจะต้องสัมพันธ์กับการเก็บข้อมูลใน Block

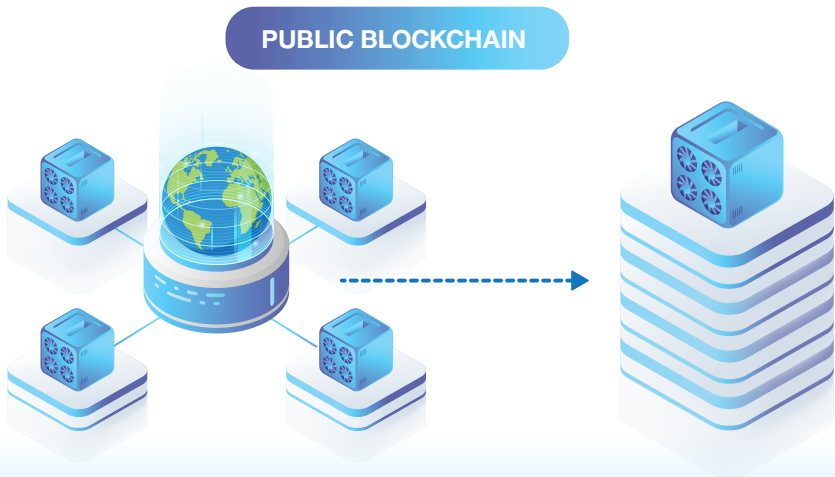
ประเภทของ Blockchain

Blockchain สามารถแบ่งออกได้เป็น 3 ประเภท โดยพิจารณาจากข้อกำหนดในการเข้าร่วมเป็นสมาชิกของเครือข่าย คือ Blockchain แบบเปิดสาธารณะ (Public Blockchain) Blockchain แบบปิด (Private Blockchain) และ Blockchain แบบเฉพาะกลุ่ม (Consortium Blockchain)



Public Blockchain

Public Blockchain คือ Blockchain วงเปิดที่อนุญาตให้ทุกคนสามารถเข้าใช้งานไม่ว่าจะเป็นการอ่าน หรือการทำธุรกรรมต่าง ๆ ได้อย่างอิสระ โดยไม่จำเป็นต้องขออนุญาต หรือรู้จักกันในอีกชื่อ คือ Permissionless Blockchain ดังแสดงในรูปภาพที่ 9



รูปภาพที่ 9: Public Blockchain

ที่มา: ปรับปรุงจาก (Kohut, 2018)



โดยทุกคนในเครือข่ายสามารถเห็นข้อมูลรายการธุรกรรมได้ ซึ่งรายการธุรกรรมที่เกิดขึ้นใหม่จะต้องผ่านกระบวนการทำ Consensus จากสมาชิกในเครือข่ายเสียก่อน ตัวอย่างของระบบ Blockchain แบบเปิดสาธารณะ ยกตัวอย่างเช่น Bitcoin, Ethereum

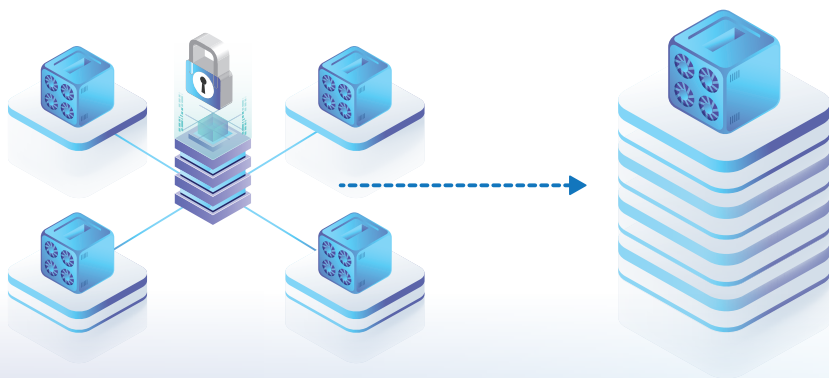




Private Blockchain

Private Blockchain คือ Blockchain วงปิดที่เข้าใช้งานได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น ซึ่งส่วนใหญ่ถูกสร้างขึ้นเพื่อใช้งานภายในองค์กร ดังนั้น ข้อมูลการทำธุรกรรมต่าง ๆ จะถูกจำกัดอยู่เฉพาะภายในเครือข่ายซึ่งประกอบไปด้วยสมาชิกที่ได้รับอนุญาตเท่านั้น ดังแสดงในรูปภาพที่ 10

PRIVATE BLOCKCHAIN



รูปภาพที่ 10: Private Blockchain

ที่มา: ปรับปรุงจาก (Kohut, 2018)

โดยภายในเครือข่ายจะมี Node หลักคอยทำหน้าที่เป็นผู้ตัดสินใจเลือกเกณฑ์สำหรับการตรวจสอบความถูกต้อง รวมถึงการบันทึกและการทำธุรกรรมของทุก Node ซึ่งผู้เข้าร่วมในกลุ่มสามารถตกลงที่จะเปลี่ยนแปลงเกณฑ์สำหรับตรวจสอบและบันทึกรายการได้ จึงเหมาะสมสำหรับการประยุกต์ใช้เพื่อเก็บข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ต้องการเผยแพร่ให้ผู้ไม่เกี่ยวข้องภายนอกองค์กรทราบ อย่างไรก็ตามหน่วยงานที่มีการสร้าง Blockchain แบบปิดเป็นของตนเอง จำเป็นต้องมี



การลงทุนในด้านโครงสร้างพื้นฐานของอุปกรณ์ ระบบเครือข่ายในการเชื่อมต่อองค์ความรู้เกี่ยวกับระบบ Blockchain ที่นำมาใช้งาน รวมทั้งการดูแลรักษา เพื่อให้ระบบสามารถดำเนินการต่อไปได้อย่างมีประสิทธิภาพ ซึ่งโดยส่วนมากมักใช้ในงานระหว่างองค์กรธุรกิจหรือระหว่างองค์กรภาครัฐ ตัวอย่างของระบบ Blockchain แบบปิด ยกตัวอย่างเช่น Hyperledger, Corda, Tendermint



Consortium Blockchain

Consortium Blockchain คือ Blockchain ที่เปิดให้ใช้งานได้เฉพาะกลุ่มเท่านั้น โดยเป็นการผสมผสานแนวคิดระหว่าง Public Blockchain และ Private Blockchain ซึ่งส่วนมากเป็นการรวมตัวกันขององค์กรที่มีลักษณะธุรกิจเหมือนกัน และต้องมีการแลกเปลี่ยนข้อมูลระหว่างกันอย่างสม่ำเสมออยู่แล้ว มารวมตัวกันตั้งวง Blockchain ขึ้นมา ทั้งนี้เนื่องจากธุรกรรมและข้อมูลที่จัดเก็บ เป็นข้อมูลที่เป็นความลับ หรือข้อมูลส่วนตัวภายในองค์กร ส่งผลให้ไม่สามารถเปิดเผยข้อมูลดังกล่าวทั้งหมดแก่สาธารณชนได้ ดังนั้นผู้เข้าร่วม Blockchain เฉพาะกลุ่ม จำเป็นต้องได้รับการอนุญาตจากตัวแทนเสียก่อน จึงจะสามารถเข้าใช้งานได้ ยกตัวอย่างเช่น เครือข่ายระหว่างธนาคาร ที่ใช้ในการแลกเปลี่ยนข้อมูลการทำธุรกรรม หรือแลกเปลี่ยนสินทรัพย์ภายในกลุ่มของธนาคาร ยกตัวอย่างเช่น Japanese Bank และ R3CEV (Buterin, 2014)

ตารางที่ 1: ตารางเปรียบเทียบคุณสมบัติของเทคโนโลยี Blockchain ในแต่ละประเภท

คุณลักษณะ (Characteristic)	Private Permitted (Private Blockchain)	Public Permitted: Single Industry	Public Permitted: Multi-Industry	Permissionless (Public Blockchain)
ผู้มีอำนาจ (Authority), การควบคุม (Control) และความน่าเชื่อถือ (Trust)	การบริหารจัดการบัญชีแยกประเภทภายในเพียงองค์กรเดียว (Centralized Trust)	การจัดการบัญชีแยกประเภทโดยมีประโยชน์อุตสาหกรรมเป็นสำคัญและเปิดใช้กับรูปแบบสาธารณะอย่างจำกัดภายในอุตสาหกรรม (Semi-Centralized Trust)	การจัดการบัญชีแยกประเภทโดยมีประโยชน์อุตสาหกรรมเป็นสำคัญ และเปิดการใช้แบบสาธารณะ (Semi-Centralized Trust)	การจัดการบัญชีแยกประเภทโดยเครือข่ายแบบกระจายศูนย์ไม่มีระบบข้อมูลกลาง (Distributed Consensus)
บริบททางธุรกิจ (Business Context)	การใช้งานภายในองค์กรเท่านั้น (Intra-Company)	การใช้งานระหว่างบริษัทหรือภายในอุตสาหกรรม (Inter-Company)	การใช้งานระหว่างบริษัทหรือข้ามอุตสาหกรรม (Inter-Company)	บริษัทและบุคคลทั่วไปสาธารณะที่อยู่ระหว่างเครือข่ายหรือระบบนิเวศของ Blockchain (Inter-Entity)
สิทธิ์การเข้าถึง (Access Rights)	การอนุญาตสิทธิ์การใช้งานวัตถุประสงค์เดียวของหนึ่งองค์กร	การอนุญาตให้ใช้สิทธิ์ในอุตสาหกรรมเดียว	การกำหนดสิทธิ์ในอุตสาหกรรม/วัตถุประสงค์หลายแบบ	อนุญาตให้ผู้เข้าร่วมหลายอุตสาหกรรม/ผู้เข้าร่วมการศึกษาค้นคว้าและผู้ที่ต้องการใช้งานหลายประเภท

คุณลักษณะ: (Characteristic)	Private Permissioned (Private Blockchain)	Public Permissioned: Single Industry	Public Permissioned: Multi-Industry	Permissionless (Public Blockchain)
การเป็นสมาชิก (Membership)	Static	Static	Semi-Static	Fluid
ความรับผิดชอบ (Accountability), สถานะทาง กฎหมาย (Legal Standing)	ผู้รับผิดชอบ ตามกฎหมาย	ผู้ที่รับผิดชอบ ตามกฎหมาย และอาจได้รับ การควบคุม	ผู้ที่รับผิดชอบ ตามกฎหมาย และอาจได้รับ การควบคุม	ผู้ที่รับผิดชอบ จำกัด/ไม่มี กฎหมายรับรอง และผู้ใช้ ไม่ได้รับ การควบคุม
รูปแบบการนำ ไปใช้ (Deployment Style)	อาจแก้ไขได้	กึ่งสามารถ แก้ไขได้	กึ่งสามารถ แก้ไขได้	ส่วนใหญ่ ไม่สามารถ แก้ไขได้
รูปแบบการ บันทึก ความไม่ เปลี่ยนแปลง (Record Immutability)	อาจแก้ไขได้	กึ่งสามารถ แก้ไขได้	กึ่งสามารถ แก้ไขได้	ส่วนใหญ่ ไม่สามารถ แก้ไขได้
Consensus Mechanism	Proof of Stake, Federated Byzantine Fault Tolerance Agreement, Proof of Authority, Proof of Identity	Proof of Stake, Practical Byzantine Fault Tolerance, Deposit-Based, Federated Byzantine Agreement	Proof of Stake, Practical Byzantine Fault Tolerance, Deposit-Based, Federated Byzantine Agreement	Proof of Work
	(Ethereum Kovan Testnet, POA Chain, R3 (Banks), EWF (Energy), B3i (Insurance), Corda)			(Bitcoin, Ethereum, etc..)

คุณลักษณะ: (Characteristic)	Private Permissioned (Private Blockchain)	Public Permissioned: Single Industry	Public Permissioned: Multi-Industry	Permissionless (Public Blockchain)
ข้อดี (Advantages)	<ol style="list-style-type: none"> 1. การรับรองความถูกต้องและการรักษาความปลอดภัยด้วยสิทธิของผู้ใช้ที่ไว้วางใจได้อย่างน่าเชื่อถือ 2. การปรับปรุงหรือเพิ่มประสิทธิภาพของโปรโตคอลและเครือข่ายได้ 3. ค่าใช้จ่ายในการจัดการระบบเครือข่ายและการจัดการใช้งานร่วมกัน 4. การกำกับดูแลและการบังคับใช้นโยบาย 5. การกำกับดูแลกฎระเบียบ 6. การพัฒนามาตรฐานและการควบคุม 7. ความสามารถในการทำงานที่รวดเร็วขึ้น 8. การปกป้องข้อมูล สินค้า บริการ หรือกลยุทธ์ทางธุรกิจ ให้มีเสถียรภาพมั่นคงและปลอดภัย 			<ol style="list-style-type: none"> 1. ข้อมูลทั้งหมดจะเป็นข้อมูลสาธารณะ 2. ความสามารถในการป้องกัน การถูกโจมตี 3. ไม่มีศูนย์กลางในการควบคุม (No Centralized) 4. ไม่มีการแยกผู้ใช้ ออกจากนักพัฒนา Application 5. การเติบโตของระบบนิเวศผ่านทางเครือข่าย 6. โอเพ่นซอร์ส (Opensource) 7. การมีนักพัฒนาซอฟต์แวร์ ร่วมกันพัฒนา

คุณลักษณะ: (Characteristic)	Private Permissioned (Private Blockchain)	Public Permissioned: Single Industry	Public Permissioned: Multi-Industry	Permissionless (Public Blockchain)
ข้อเสีย (Disadvantages)	<ol style="list-style-type: none"> จุดเดียวของความล้มเหลว (Single Point of Failure) อาจไม่สามารถเปิดแหล่งที่มาได้ การเสริมสร้างรูปแบบธุรกิจ และชุดกระบวนการที่มีอยู่ การที่ต้องดูแลระบบและค่าใช้จ่ายต่าง ๆ ผู้จัดทำเป็นศูนย์กลางข้อมูลกลาง (ในกรณีผู้ซื้อหรือลูกค้าเป็นศูนย์กลาง) การจัดการทรัพยากรบุคคลสำหรับพัฒนาซอฟต์แวร์ ที่มีอยู่จำกัด การใช้งานต้องมีมติหรือข้อตกลงเป็นเอกฉันท์ขององค์กร 			<ol style="list-style-type: none"> ปัญหาความสามารถในการรองรับการปรับขยายขนาดธุรกรรมทำให้เกิดความล่าช้าในการทำธุรกรรม การกำกับดูแลที่ซับซ้อน การมีส่วนร่วมของผู้เกี่ยวข้องที่ไม่น่าเชื่อถือ ศักยภาพในการตรวจสอบธุรกรรม (Minner) ศักยภาพบางประการที่อาจผิดกฎหมาย สิ่งจูงใจทางการเงินที่ต้องใช้เพื่อรักษาเครือข่าย

ที่มา: ปรับปรุงจาก (Zheng, Xie, Dai, & Wang, 2016)

คุณลักษณะพื้นฐานที่สำคัญของเทคโนโลยี Blockchain

การจัดเก็บข้อมูลในรูปแบบของ Block โดยเชื่อมต่อแต่ละ Block ด้วย Hash Function และกระจายให้ทุก ๆ Node เก็บ ทำให้เกิดคุณสมบัติที่สำคัญของ Blockchain 3 ประการ คือ ความถูกต้องเที่ยงตรงของข้อมูล (Data Integrity) ความโปร่งใสในการเข้าถึงข้อมูล (Data Transparency) และความสามารถในการทำงานได้อย่างต่อเนื่องของระบบ (Availability) (Serrano, 2017)



ความถูกต้องเที่ยงตรงของข้อมูล (Data Integrity)

เนื่องจากการเชื่อมโยง Block ปัจจุบันและ Block ก่อนหน้าด้วย Hash Function และทำการกระจายให้ทุก Node เก็บ ทำให้ข้อมูลที่ถูกรับที่ลงใน Blockchain แล้วไม่สามารถแก้ไข หรือเปลี่ยนแปลงข้อมูลได้ (Immutability) ดังนั้นหากมีความพยายามในการแก้ไขหรือเปลี่ยนแปลงข้อมูลที่ถูกรับที่ลงใน Block แล้วจะทำให้ทราบได้ทันทีเนื่องจากข้อมูลใน Node ดังกล่าวจะมีข้อมูลที่ต่างออกไปจาก Node อื่น ๆ ในระบบ และไม่สามารถสร้าง Consensus กับ Node อื่นได้ ทำให้ถูกแยกออกจาก Chain หลักไปในที่สุด



ความโปร่งใสในการเข้าถึงข้อมูล (Data Transparency)

เนื่องจากทุก Node ในระบบ Blockchain จะเก็บข้อมูลเดียวกันทั้งหมด โดยไม่มี Node ใด Node หนึ่งเป็นตัวกลางที่มีอำนาจแต่เพียงผู้เดียวในการเก็บข้อมูล ดังนั้นการเข้าถึงข้อมูลใด ๆ จึงทำได้จาก Node ตัวเองทันที โดยไม่จำเป็นต้องร้องขอข้อมูลจากตัวกลาง จึงเรียกว่าเป็นระบบที่มีความโปร่งใสในการเข้าถึงข้อมูลสูงมาก



ความสามารถในการทำงานได้อย่างต่อเนื่องของระบบ (Availability)

เนื่องจากทุก Node ในระบบ Blockchain จะเก็บข้อมูลเดียวกันทั้งหมด จึงสามารถทำงานทดแทนกันได้เมื่อมี Node ที่ไม่สามารถให้บริการได้ในขณะนั้น โดยระบบจะทำการคัดลอกสำเนาข้อมูลให้เป็นข้อมูลชุดเดียวกันเมื่อ Node กลับขึ้นมาให้บริการได้อีกครั้ง



เกณฑ์การพิจารณาเลือกใช้เทคโนโลยี Blockchain

เกณฑ์ในการพิจารณาเลือกใช้เทคโนโลยี Blockchain เพื่อพิจารณาความเหมาะสม และความจำเป็นในมิติต่าง ๆ ตามข้อคำถามทั้ง 6 คำถาม สำหรับใช้ในการตัดสินใจเพื่อให้องค์กรสามารถเลือกใช้เทคโนโลยี Blockchain ได้อย่างเหมาะสม อีกทั้งยังสามารถนำเทคโนโลยี Blockchain มาใช้เพื่อแก้ปัญหาการทำงานในอดีต และก่อให้เกิดประโยชน์ต่อการวางแผนการทำงานในอนาคตได้ ดังแสดงในรูปภาพที่ 11



รูปภาพที่ 11: กระบวนการตัดสินใจก่อนการนำเทคโนโลยี Blockchain มาใช้งาน

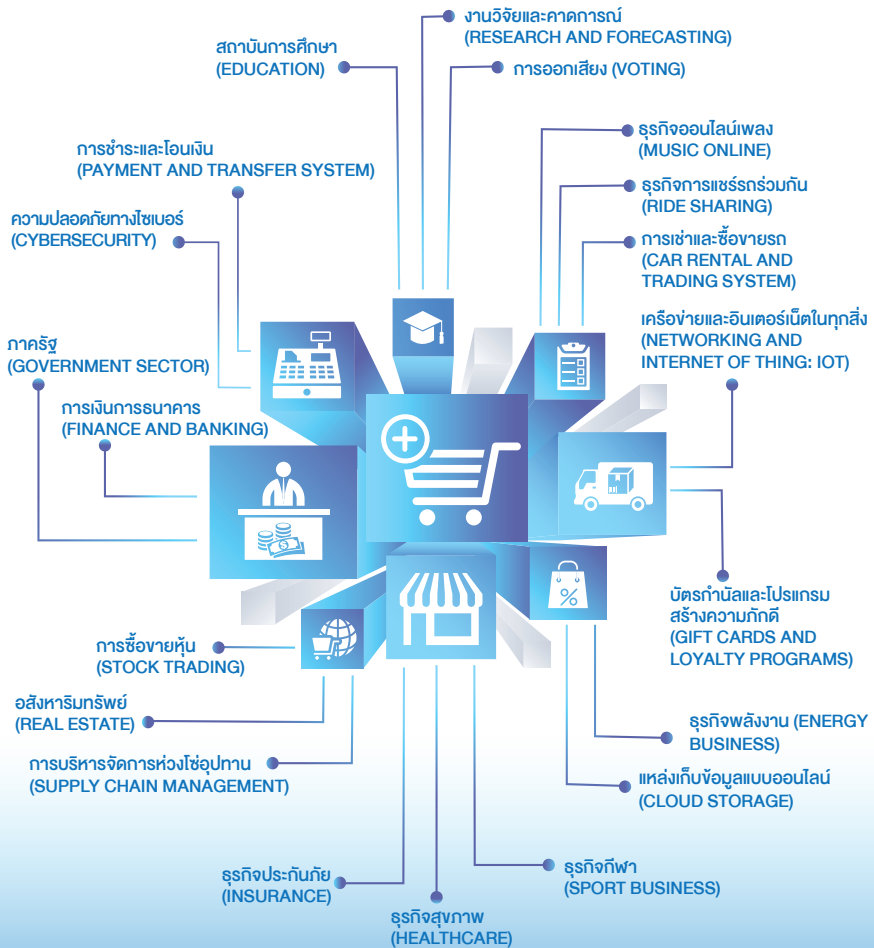
ที่มา: ปรับปรุงจาก (Yaga, Mell, Roby, & Scarfone, 2018a)

รูปแบบการประยุกต์ใช้เทคโนโลยี Blockchain



ในปัจจุบันเทคโนโลยี Blockchain ถือได้ว่าอยู่ในช่วงเริ่มต้นของการนำไปใช้งาน โดยอ้างอิงข้อมูลจาก World Economic Forum Survey (2015) พบว่ามูลค่ารวมของธุรกรรมที่มีการใช้งานอยู่บนเทคโนโลยี Blockchain รวมไปถึง Bitcoin นั้นยังมีปริมาณค่อนข้างน้อยเมื่อเทียบกับ GDP ของโลก โดยมีปริมาณเพียง 0.025% หรือคิดเป็นมูลค่าประมาณสองหมื่นล้านเหรียญสหรัฐนั่นเอง (Global GDP มีมูลค่า 80 ล้านล้านเหรียญสหรัฐ) แต่จากรายงาน ได้แสดงให้เห็นว่าการใช้งานเทคโนโลยี Blockchain มีแนวโน้มจะเป็นไปอย่างก้าวกระโดดภายใน 10 ปีนี้ เนื่องจากภาคธุรกิจต่าง ๆ ได้เห็นถึงประโยชน์และความสำคัญของการนำเทคโนโลยี Blockchain ไปใช้งาน โดยในปี 2015 มีตัวเลขการลงทุนในธุรกิจที่เกี่ยวข้องกับเทคโนโลยี Blockchain สูงถึง 474 ล้านดอลลาร์สหรัฐซึ่งโตขึ้น

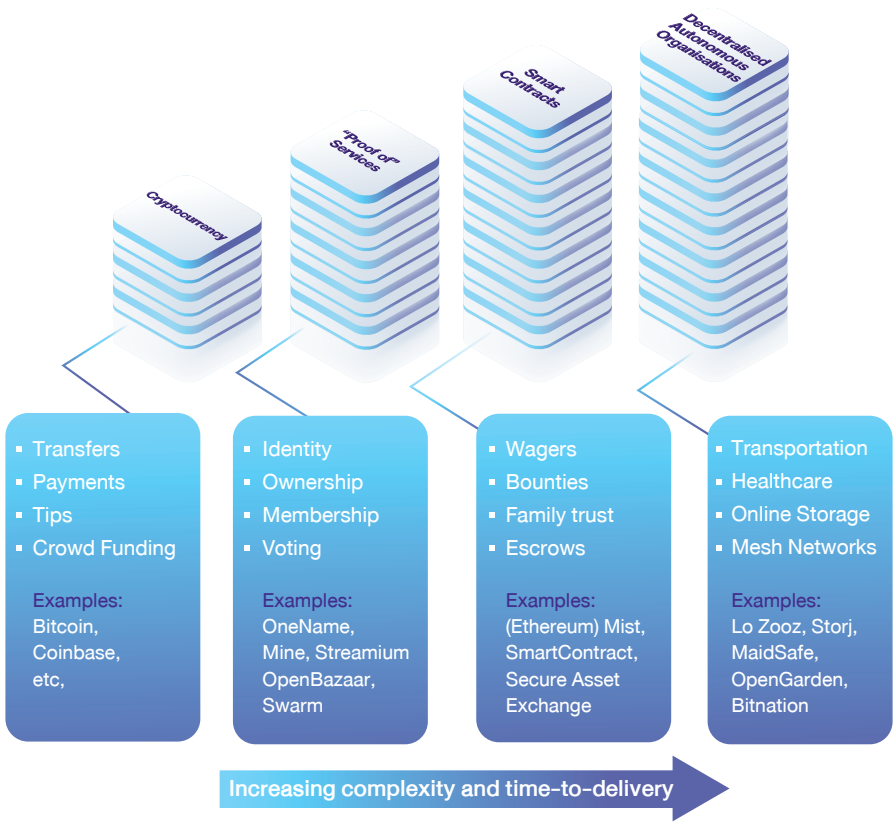
ถึง 59% จากปีก่อนหน้านี้ โดยในปัจจุบันได้มีการนำเทคโนโลยี Blockchain มาใช้งานกันอย่างกว้างขวางมากขึ้นไม่จำเพาะแค่เพียงภาคการเงินและการธนาคาร เท่านั้น ดังแสดงในรูปภาพที่ 12 ไม่ว่าจะเป็นธุรกิจ Supply Chain ธุรกิจประกันภัย ธุรกิจเกี่ยวกับสุขภาพสถาบันการศึกษา หรือแม้แต่วิจิธุรกิจเพลงออนไลน์ รวมไปถึงภาครัฐก็ได้ให้ความสนใจเกี่ยวกับการทำเทคโนโลยี Blockchain ไปใช้ในการบริหาร งานภาครัฐกันมากขึ้นเช่นกัน



รูปภาพที่ 12: การประยุกต์ใช้เทคโนโลยี Blockchain ในภาคส่วนต่าง ๆ

ดังนั้นจากข้อมูลการประยุกต์ใช้เทคโนโลยี Blockchain ในภาคส่วนต่าง ๆ ดังได้กล่าวมาแล้วข้างต้นทำให้สามารถจัดกลุ่มการพัฒนา Application ที่ทำงานอยู่บนพื้นฐานของเทคโนโลยี Blockchain ได้เป็น 4 กลุ่มดังแสดงในรูปภาพที่ 13

Key Blockchain Application Groupings



รูปภาพที่ 13: การจำแนกกลุ่ม Blockchain Application

ที่มา: ปรับปรุงจาก (Umeh, 2016)



เงินดิจิทัล (Cryptocurrency)

สกุลเงินดิจิทัลซึ่งมีมูลค่าเหมือนกับธนบัตรในสกุลเงินประเทศต่าง ๆ และถูกใช้เป็นสื่อกลางในการแลกเปลี่ยนแบบดิจิทัล โดยการแลกเปลี่ยนรูปแบบดิจิทัลได้เริ่มขึ้นเมื่อปี ค.ศ. 2009 ซึ่ง Blockchain Application ในกลุ่มเงินดิจิทัลได้ถูกพัฒนาขึ้นเพื่อใช้ในธุรกิจการให้บริการทางการเงินทั้งการโอนและการจ่ายเงิน ยกตัวอย่างเช่น Bitcoin และ Ripple



บริการพิสูจน์ทราบ (Proof of Services)

การบริการพิสูจน์ทราบ คือ การประยุกต์ใช้เทคโนโลยี Blockchain ในการบรรจุข้อมูลแบบอัตโนมัติ ยกตัวอย่างเช่น การเก็บข้อมูลเอกลักษณ์ (Identity) กรรมสิทธิ์ (Ownership) และสมาชิกภาพ (Membership) ซึ่งส่วนใหญ่ Application ดังกล่าวมักจะถูกนำไปประยุกต์ใช้โดยหน่วยงานภาครัฐ ซึ่งทำหน้าที่เกี่ยวกับการบริการประชาชน ยกตัวอย่างเช่น MIT Digital Currency Initiative ได้ร่วมมือกับหลายภาคส่วนรวมไปถึงภาครัฐเพื่อสร้างโครงการนำร่องเกี่ยวกับการใช้งานเทคโนโลยี Blockchain ในการออกใบสูติบัตร ใบมรณะบัตร ใบอนุญาตประกอบธุรกิจ ชื่อสถานประกอบการ รวมไปถึงวุฒิการศึกษา ซึ่งในหลาย ๆ โครงการได้มีการพัฒนาจนเป็นรูปธรรม และได้มีการนำไปใช้จริงแล้ว ยกตัวอย่างเช่น บริการยืนยันเอกลักษณ์ (Identity Based Service) โดย BitNation มีจุดมุ่งหมายเพื่อกระจายการอำนาจการกำกับดูแลในระดับโลก ได้ทำการพัฒนา A World Citizenship ID บน Blockchain Protocol (Umeh, 2016)



นอกจากนี้ยังมี Proof of Service อีกประเภทหนึ่งหรือที่รู้จักกันในชื่อ Proof of Existence คือการพิสูจน์การมีอยู่จริงของเอกสารต่าง ๆ โดยหลักการ คือ การเก็บข้อมูลโดยสรุปของเอกสารที่สามารถยืนยันการมีอยู่จริงของข้อมูลภายใน เอกสารต้นฉบับได้ หรือที่เรียกว่า Cryptographic Digest รวมไปถึงเวลาที่จัดส่ง เอกสารไปยังผู้รับซึ่งข้อมูลดังกล่าวจะถูกจัดเก็บลงใน Blockchain ดังนั้นผู้ใช้งาน มั่นใจได้ว่าเอกสารที่ได้รับนั้นเป็นเอกสารที่ถูกต้องและเชื่อถือได้ อีกทั้งไม่จำเป็นต้องกังวลเกี่ยวกับความเป็นส่วนตัวเนื่องจากข้อมูลที่ถูกจัดเก็บลงใน Blockchain เป็นเพียงข้อมูลโดยสรุปของเอกสารที่สามารถยืนยันการมีอยู่จริงของข้อมูลภายใน เอกสารต้นฉบับได้ และเวลาที่จัดส่งเอกสารไปยังผู้รับเท่านั้นไม่ใช่เอกสารต้นฉบับ



สัญญาอัจฉริยะ: (Smart Contract)

สัญญาอัจฉริยะ คือ โปรแกรมคอมพิวเตอร์ที่สามารถดำเนินการตามข้อตกลงโดยอัตโนมัติทันทีที่เกิดเหตุการณ์ตามเงื่อนไขในสัญญาซึ่งได้มีการระบุถึงเงื่อนไข หรือเหตุการณ์ดังกล่าวไว้ล่วงหน้าแล้ว โดยไม่ต้องมีคนกลาง นั่นคือหลักการสำคัญของสัญญาอัจฉริยะ ซึ่งได้ถูกคิดค้นขึ้นในปี 1994 โดย Nick Szabo (Crosby, Pattanayak, Verma, & Kalyanaraman, 2016) ยกตัวอย่างเช่น การโอนเงินจ่ายค่าลิขสิทธิ์ซอฟต์แวร์อัตโนมัติ ทันทีที่จำนวนผู้ใช้ถึงระดับที่ตกลงกับเจ้าของลิขสิทธิ์ซอฟต์แวร์ไว้ล่วงหน้า การโอนเงินจ่ายค่าโฆษณาบนเว็บไซต์โดยอัตโนมัติ ทันทีที่จำนวนคนดูถึงระดับที่ตกลงกับเจ้าของเว็บไซต์ การโอนคูปองส่วนลดราคาสินค้ามาให้ลูกค้าอัตโนมัติ ทันทีที่ถึงวันที่ใช้คูปองนั้นได้ หรือแม้แต่การโอนเงินจ่ายค่าบทความ ทันทีและทุกครั้งที่จำนวนผู้อ่านบทความถึงระดับที่ตกลงกับนักเขียนไว้ล่วงหน้า トラบโดที่คู่สัญญาทุกฝ่ายตกลงกันได้ เมื่อนั้นสัญญาอัจฉริยะ หรือ Smart Contract ก็จะถูกโปรแกรมและบริหารจัดการอัตโนมัติด้วยโปรแกรมคอมพิวเตอร์บนเทคโนโลยี Blockchain ซึ่งในปัจจุบันบริษัท Ethereum และ Codius ได้เปิดใช้งาน Smart Contract บนพื้นฐานของเทคโนโลยี Blockchain โดย The Ethereum Project เป็นหนึ่งตัวอย่างของการทำ Smart Contract เต็มรูปแบบซึ่งอยู่ในรูปแบบของ Public Blockchain ส่วนตัวอย่างอื่น ๆ นั้นเป็นการทำ Smart Contract ในรูปแบบของ Private หรือ Permissioned Blockchain ซึ่งจะทำการติดต่อเฉพาะ Node ที่รู้จักและเชื่อถือได้เท่านั้น เพื่อเพิ่มความปลอดภัย การนำสัญญาอัจฉริยะ หรือ Smart Contract มาใช้งานนั้นสามารถช่วยแก้ปัญหาความไม่ไว้วางใจกันระหว่างคู่สัญญา การฉ้อโกง และการบิดเบือนสัญญา อีกทั้งยังสามารถช่วยแก้ปัญหาการตีความเนื้อหาในสัญญา ซึ่งมักจะเป็นข้อพิพาทระหว่างคู่สัญญาเสมอ ๆ เนื่องจากคู่สัญญาทั้งสองฝ่ายต่างตีความสัญญาคนละแบบ

ทั้งนี้ในการประยุกต์ใช้งาน Smart Contract ร่วมกับกระบวนการต่าง ๆ ที่เกี่ยวข้อง จำเป็นต้องทราบจุดเด่น และข้อจำกัดของ Smart Contract ที่เกี่ยวข้อง เพื่อให้สามารถนำ Smart Contract ไปใช้งานได้อย่างเหมาะสม โดยจุดเด่นของ Smart Contract ประกอบไปด้วย



ความปลอดภัย (Security) เนื่องจาก Smart Contract ที่ถูกพัฒนาโดยใช้เทคโนโลยี Blockchain นั้นจะถูกกระจายไปยังสมาชิกอื่น ๆ ที่อยู่ในเครือข่าย จึงมั่นใจได้ว่า Smart Contract ดังกล่าวจะไม่สูญหาย หรือถูกเปลี่ยนแปลงเงื่อนไขการทำงานโดยไม่ได้รับอนุญาต



ความเป็นอัตโนมัติ (Automation) เนื่องจาก Smart Contract จะดำเนินการตามข้อตกลงโดยอัตโนมัติทันทีเมื่อเกิดเหตุการณ์ตามเงื่อนไขในสัญญา ซึ่งได้มีการระบุไว้ล่วงหน้าแล้ว โดยไม่ต้องมีคนกลางมาเกี่ยวข้อง



ความเป็นมาตรฐาน (Standardization) เนื่องจาก การนำ Smart Contract มาใช้งานในระบบใด ๆ นั้น หมายความว่าระบบนั้นจะต้องทำงานภายใต้เงื่อนไข หรือข้อตกลงต่างที่เป็นมาตรฐานเดียวกันทั้งระบบ ตามที่ได้กำหนดไว้ใน Smart Contract





ดังนั้นจากจุดเด่นของ Smart Contract ดังได้กล่าวมาแล้วข้างต้นลักษณะงานที่เหมาะสมสำหรับการนำ Smart Contract ไปประยุกต์ใช้ ประกอบไปด้วย



งานที่เกี่ยวข้องกับข้อมูลที่ไม่ต้องการให้แก้ไขได้ หรือสามารถเปลี่ยนแปลงเพิ่มเติมได้จากผู้ที่ได้รับอนุญาตเท่านั้น ยกตัวอย่างเช่น การเก็บข้อมูลสำหรับใช้ยืนยันบุคคล การเก็บข้อมูลสินทรัพย์ที่มีมูลค่าต่าง ๆ



งานที่ต้องการให้ธุรกรรมสามารถดำเนินการได้อย่างอัตโนมัติตามเงื่อนไขที่กำหนด โดยปราศจากตัวกลางในการควบคุม หรือกำหนดการตัดสินใจ ยกตัวอย่างเช่น งานเกี่ยวกับการแลกเปลี่ยนสินทรัพย์



งานที่จำเป็นต้องเก็บประวัติการทำธุรกรรมที่เกี่ยวข้อง เพื่อใช้ในการสืบข้อมูลย้อนกลับ หรือตรวจสอบความถูกต้อง ยกตัวอย่างเช่น งานเก็บประวัติการรักษาทางการแพทย์ งานเก็บประวัติข้อมูลการถ่ายโอนสินทรัพย์ที่มีมูลค่า



งานที่ต้องการลดค่าใช้จ่ายกรณีมีตัวกลางร่วมในการบริหารจัดการระบบ ซึ่งสามารถประยุกต์ใช้ได้กับหลายหน่วยงานที่มีการใช้บุคลากร หรือสาขาของสำนักงานในการดำเนินงานเป็นจำนวนมาก

ถึงแม้ Smart Contract จะมีจุดเด่นและความเหมาะสมกับการนำไปใช้ในงานประเภทต่าง ๆ ดังได้กล่าวมาแล้วข้างต้น แต่อย่างไรก็ดีหากมีการนำ Smart Contract ไปใช้งาน ก็ยังจำเป็นที่จะต้องพิจารณาข้อจำกัดดังต่อไปนี้ร่วมด้วย



ความผิดพลาดที่เกิดจากมนุษย์ (Human Error) เนื่องจากการสร้าง Smart Contract คือ การเขียนโปรแกรม และกำหนดขั้นตอนการทำงาน ดังนั้นหากมีการทดสอบไม่เพียงพอ Smart Contract ที่สร้างขึ้นสามารถทำงานผิดพลาดได้ โดยความผิดพลาดที่เกิดขึ้นอาจสร้างความเสียหายและส่งผลกระทบต่อวงกว้าง



ความยากต่อการเปลี่ยนแปลง (Immutable) หรือปรับปรุงเวอร์ชันของ Smart Contract เนื่องจาก Smart Contract และข้อมูลที่เกี่ยวข้องได้ทำการลงทะเบียน และมีการเชื่อมต่อกับระบบที่เกี่ยวข้องเรียบร้อยแล้ว ดังนั้นหากมีการเปลี่ยนแปลง Smart Contract ส่งผลให้ต้องมีการเปลี่ยนแปลงการเชื่อมต่อกับระบบที่เกี่ยวข้องใหม่ทั้งหมด



ความเชื่อมั่น (Confidence) เนื่องจากในปัจจุบันยังขาดการรับรองด้านกฎหมายที่เกี่ยวข้องกับการจัดการธุรกรรมผ่าน Smart Contract



ค่าใช้จ่าย (Cost) เนื่องจากการพัฒนา Smart Contract และส่วนเชื่อมต่อกับระบบอื่นที่เกี่ยวข้อง จำเป็นต้องใช้บุคลากรที่มีประสบการณ์สูงในการดำเนินการดังกล่าว ส่งผลให้ค่าใช้จ่ายในการดำเนินการสำหรับกระบวนการดังกล่าวสูงขึ้นตามไปด้วย



ระบบ/บริการอัตโนมัติ (Decentralized Autonomous Systems/Services)

ระบบ/บริการอัตโนมัติ ถูกมองว่าเป็นพัฒนาการขั้นสูงสุดสำหรับการพัฒนา Application บนเทคโนโลยี Blockchain คือ การทำให้คอมพิวเตอร์สามารถคุยกันเองเพื่อบริหารกิจการได้เองแบบอัตโนมัติ โดยไม่ต้องอาศัยการตัดสินใจของมนุษย์ หรือไม่ต้องมีมนุษย์เข้ามาเกี่ยวข้อง ที่เรียกว่า “องค์กรอัตโนมัติกระจายศูนย์ (Decentralized Autonomous Organization: DAO) โดยการแปลงสัญญาและข้อตกลงทั้งหมดขององค์กรหรืออะไรก็ตามให้อยู่ในรูปแบบของ “สัญญาอัจฉริยะ (Smart Contracts)” แต่อย่างไรก็ดี สัญญาอัจฉริยะ (Smart Contracts) ก็เป็นเพียงแค่ชุดคำสั่งทางคอมพิวเตอร์เท่านั้น ซึ่งในทางปฏิบัติไม่ได้มีศักยภาพใด ๆ ที่จะทำหน้าที่ในการผลิตสินค้า เขียนโค้ด หรือวาดถนน ดังนั้นการที่องค์กรอัตโนมัติกระจายศูนย์ (Decentralized Autonomous Organization: DAO) จะเกิดผลสัมฤทธิ์ในเชิงปฏิบัติได้นั้น





จึงจำเป็นต้องมี “ผู้รับเหมา (Contractor)” โดย DAO จะเปิดให้ใครก็ได้ส่ง “ข้อเสนอ” (Proposal) ที่จะพัฒนา/ผลิตสินค้าหรือบริการเข้ามา ข้อเสนอเหล่านี้ต้องอยู่ในรูปของสัญญาอัจฉริยะ (Smart Contract) แนบด้วยข้อเสนอในรูปภาษาธรรมดา จากนั้นข้อเสนอดังกล่าว จะถูกตรวจสอบว่าขัดแย้งกับผลประโยชน์ของ DAO หรือไม่ และมีคุณสมบัติครบตามที่ DAO ระบุหรือไม่ จากนั้นข้อเสนอของผู้รับเหมาที่ผ่านการพิจารณาจะถูกเติมเข้าไปในรายชื่อบัญชีที่มีสิทธิได้รับเงินจาก DAO ทั้งนี้องค์กรอัตโนมัติกระจายศูนย์ (Decentralized Autonomous Organization: DAO) เป็นสิ่งที่สามารถเกิดขึ้นได้ โดยเฉพาะเมื่อเป็นการพัฒนาควบคู่กันไประหว่างเทคโนโลยี Blockchain และปัญญาประดิษฐ์ (Artificial Intelligence: AI) (สฤณี อาชวานันทกุล (2016))



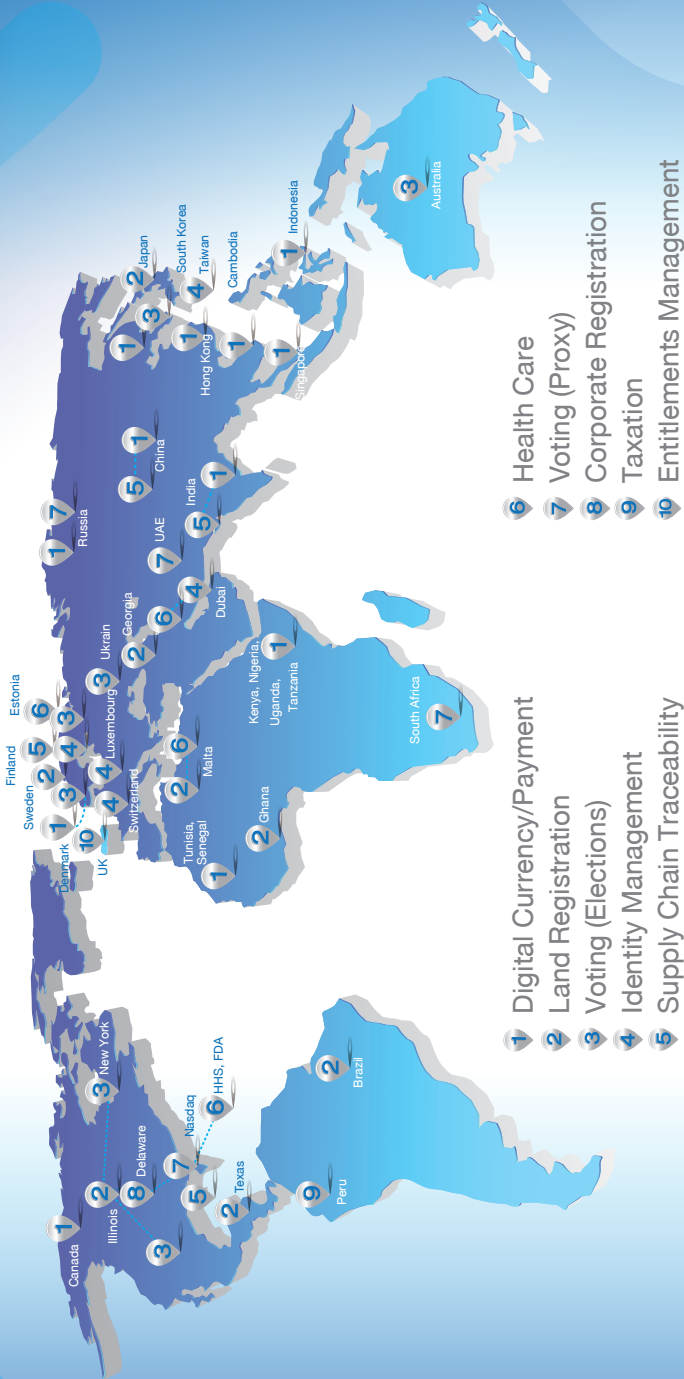
02

การประยุกต์ใช้เทคโนโลยี
Blockchain
เพื่องานบริการภาครัฐ
กรณีศึกษาต่างประเทศ

การประยุกต์ใช้เทคโนโลยี Blockchain เพื่องานบริการภาครัฐ กรณีศึกษาต่างประเทศ



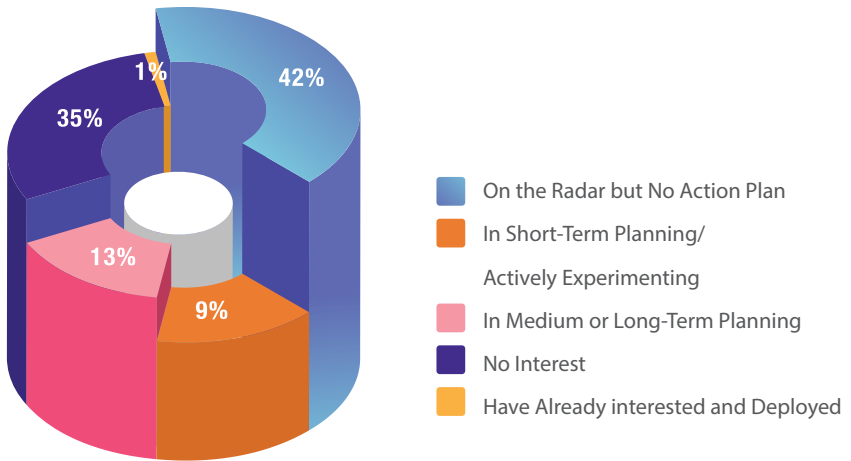
ปัจจุบันการนำเทคโนโลยี Blockchain มาใช้ในงานบริการภาครัฐมีแนวโน้มสูงขึ้นอย่างมาก โดยพบว่ามีมากกว่า 30 ประเทศทั่วโลก ยกตัวอย่างเช่น เอสโตเนีย แคนาดา อังกฤษ บราซิล จีน และอินเดีย เริ่มมีการศึกษา ทดลอง รวมไปถึงการพัฒนา จนนำไปสู่การนำเทคโนโลยี Blockchain มาใช้สำหรับงานบริการภาครัฐอย่างเป็นรูปธรรมดังแสดงในรูปภาพที่ 14 (โดยรายละเอียดการนำเทคโนโลยี Blockchain มาใช้ในงานบริการภาครัฐแยกตามประเทศ ดังปรากฏในเอกสารแนบท้ายที่ 1)



รูปถ่ายที่ 14: การประยุกต์ใช้เทคโนโลยี Blockchain สำหรับงานบริการภาครัฐของประเทศไทย

ที่มา: ปรับปรุงจาก (Deloitte, 2018)

ซึ่งมีความสอดคล้องกับรายงานผลการสำรวจความคิดเห็นของ CIO ส่วนใหญ่ ดังแสดงในรูปภาพที่ 15 พบว่าความเห็นของ CIO ส่วนใหญ่ตระหนักและให้ความสำคัญกับการนำเทคโนโลยี Blockchain มาใช้ในงานบริการภาครัฐเป็นอย่างมาก โดยพบว่า 22% ของหน่วยงานภาครัฐได้มีการวางแผนทั้งในระยะสั้นและระยะยาวในการนำเทคโนโลยี Blockchain มาใช้งาน รวมถึงมีความสนใจในการนำเทคโนโลยีดังกล่าวมาใช้งาน และอยู่ระหว่างการศึกษาความเป็นไปได้สูงถึง 42%



รูปภาพที่ 15: ผลการสำรวจความคาดหวังในการนำเทคโนโลยี Blockchain มาใช้ในภาครัฐ
ที่มา: ปรับปรุงจาก (Holgate, 2018)

ทั้งนี้วัตถุประสงค์ของการนำเทคโนโลยี Blockchain มาใช้สำหรับงานบริการภาครัฐในต่างประเทศเป็นไปเพื่อวัตถุประสงค์ดังต่อไปนี้

วัตถุประสงค์ของการนำเทคโนโลยี Blockchain มาใช้สำหรับงานบริการภาครัฐ

1

การให้ความช่วยเหลือ และการบริการประชาชน Social Welfare

ในการเข้าถึงสวัสดิการ และบริการต่าง ๆ ของภาครัฐ ด้วยคุณสมบัติของเทคโนโลยี Blockchain สามารถช่วยปรับปรุงคุณภาพระบบการลงทะเบียน (Registration System) เพื่อแจกจ่ายสวัสดิการภาครัฐให้กับประชาชนได้อย่างมีประสิทธิภาพมากยิ่งขึ้น อีกทั้งการทำงานร่วมกับระบบพิสูจน์ตัวตน (Identity Management) บนเทคโนโลยี Blockchain สามารถช่วยลดขั้นตอน และการใช้สำเนาเอกสารในการพิสูจน์ตัวตนได้ ทำให้ประชาชนได้รับความสะดวกและรวดเร็วในการได้รับบริการ ยกตัวอย่างเช่น ประเทศอังกฤษ ได้นำเทคโนโลยี Blockchain มาใช้ใน



การจ่ายเงินสวัสดิการภาครัฐต่าง ๆ โดยประชาชนจะได้รับเงินโดยตรงผ่านทาง Digital Wallet ของพวกเขา ซึ่งช่วยลดค่าธรรมเนียมธนาคาร และลดโอกาสในการทุจริตจากหน่วยงานท้องถิ่นลงได้ ทำให้เกิดความโปร่งใส และสามารถตรวจสอบการใช้จ่ายเงินของภาครัฐได้

2

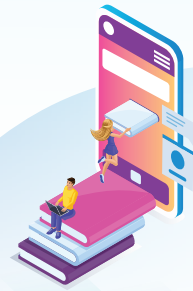
การเพิ่มประสิทธิภาพ ในการบริหารงานภาครัฐ e-Government

การนำเทคโนโลยี Blockchain มาใช้ในการบริหารงานภาครัฐ หรือที่รู้จักกันในชื่อระบบ e-Government ซึ่งเป็นแนวคิดที่รัฐบาลทั่วโลกกำลังให้ความสำคัญอยู่ในขณะนี้ สามารถช่วยให้เกิดการพัฒนารัฐบาลดิจิทัลได้อย่างเป็นรูปธรรมต่อไปในอนาคต ซึ่งจะเป็นประโยชน์ทั้งภาครัฐ และภาคประชาสังคม ในการช่วยลดต้นทุน ความยุ่งยาก ซับซ้อน และช่วยอำนวยความสะดวกให้กับประชาชนในการเข้าถึงบริการภาครัฐ อีกทั้งยังทำให้เกิดกระบวนการที่น่าเชื่อถือสำหรับการแบ่งปันข้อมูลภาครัฐ รวมถึงการพัฒนากระบวนการตรวจสอบความน่าเชื่อถือของข้อมูลภาครัฐ ทำให้เกิดความโปร่งใสตรวจสอบได้ ลดการทุจริตคอร์รัปชัน



ยกตัวอย่างเช่น ประเทศเอสโตเนีย ซึ่งได้ชื่อว่ามีระบบ e-Government ที่ดีที่สุดในโลก อีกทั้งยังเป็นประเทศแรก ๆ ที่ได้นำเทคโนโลยี Blockchain และบริการดิจิทัลมาใช้ในการบริหารประเทศแบบเต็มตัว เพื่อนำประเทศไปสู่สังคมดิจิทัล โดยการบริการภาครัฐเกือบทุกประเภทอยู่บนระบบออนไลน์ที่มีชื่อว่า e-Estonia ซึ่งประกอบไปด้วย e-Service ต่าง ๆ มากมาย เช่น e-Residency, e-Court, Electronic Land Register, Electronic Health Care Record และ i-Voting ประเทศเอสโตเนียมีการลงทุนด้านระบบ e-Government มาตั้งแต่ปี ค.ศ. 2000

โดยเริ่มจากระบบภาษีออนไลน์ (e-Tax Board) และระบบบริการจอดรถผ่านออนไลน์ (e-Parking) จนกระทั่งในปี ค.ศ. 2001 เริ่มทำโครงการ X-Road หรือทางเชื่อมข้อมูลภาครัฐ โดยทำการเชื่อมข้อมูลระหว่างหน่วยงานต่าง ๆ ในประเทศเอสโตเนียเข้าด้วยกัน และพัฒนาระบบดังกล่าวเรื่อยมาจน X-Road กลายเป็นกระดูกสันหลังสำคัญของงานบริการภาครัฐของประเทศเอสโตเนีย



BLOCKCHAIN TECHNOLOGY

3

การสร้างความโปร่งใส Transparency

ในยุคปัจจุบันรัฐบาลของหลายประเทศทั่วโลกกำลังก้าวเข้าสู่การเป็นรัฐบาลดิจิทัล โดยการนำเทคโนโลยีและนวัตกรรมมาใช้ในการบริหารประเทศกันมากขึ้น จากการเปลี่ยนแปลงดังกล่าวนำมาซึ่งความคาดหวังจากประชาชนที่ต้องการได้รับการบริการที่ดีขึ้น ทั้งในเรื่องของความสะดวกรวดเร็ว รวมถึงความโปร่งใส สามารถตรวจสอบได้ ดังนั้นนอกจากเทคโนโลยี Blockchain จะสามารถเข้ามาช่วยในเรื่องของการเพิ่มประสิทธิภาพในการบริหารงานภาครัฐ และการให้ความช่วยเหลือและการให้บริการประชาชน ในการเข้าถึงสวัสดิการและบริการของภาครัฐดังได้กล่าวมาแล้วนั้น เทคโนโลยี Blockchain ยังได้

ถูกนำมาใช้เพื่อสร้างความโปร่งใสให้กับ การดำเนินงานของภาครัฐอีกด้วย ยกตัวอย่างเช่น ประเทศญี่ปุ่น ได้นำเทคโนโลยี Blockchain มาใช้สำหรับการแลกเปลี่ยนข้อมูลในกระบวนการจัดซื้อจัดจ้างของภาครัฐ เพื่อสร้างความปลอดภัยในการแชร์ข้อมูลภาครัฐ รวมถึงเป็นการสร้างความโปร่งใส ตรวจสอบการใช้จ่ายเงินภาครัฐได้ (Chase, 2017)

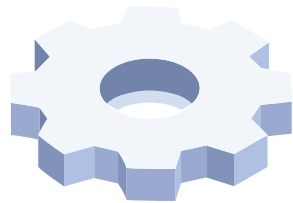


4

การรักษาความมั่นคง National Security



ปัจจุบันภัยคุกคามทางไซเบอร์ ถือได้ว่าเป็นภัยคุกคามในรูปแบบใหม่ที่สร้างผลกระทบต่อความมั่นคงของประเทศ และหนึ่งในเป้าหมายของการถูกโจมตีก็คือระบบโครงสร้างพื้นฐานที่สำคัญของประเทศ แต่ด้วยคุณสมบัติของเทคโนโลยี Blockchain ที่ยากต่อการถูกโจมตีโดยแฮกเกอร์





จึงทำให้รัฐบาลหลายประเทศสนใจ
ทำการศึกษาการนำเทคโนโลยีดังกล่าว
มาใช้เพื่อการรักษาความปลอดภัยระบบ
โครงสร้างพื้นฐานที่สำคัญของประเทศ



ยกตัวอย่างเช่น ประเทศอังกฤษได้มีการพัฒนาโครงการ Blockchain-Based Cybersecurity Services for Critical British โดยนำเทคโนโลยี Blockchain มาใช้ในการป้องกันระบบโครงสร้างพื้นฐานสำคัญของประเทศ เพื่อประโยชน์ในการรักษาความมั่นคงของชาติ

สร้างความมั่นคงปลอดภัย และความน่าเชื่อถือให้กับระบบโครงสร้างพื้นฐานที่สำคัญของประเทศ ยกตัวอย่างเช่น ระบบป้องกันน้ำท่วม ระบบควบคุมพลังงานนิวเคลียร์ รวมถึงระบบการจ่ายกระแสไฟฟ้า เป็นต้น

ประโยชน์ของการนำเทคโนโลยี Blockchain มาใช้ในงานบริการภาครัฐ

ประโยชน์ของการนำเทคโนโลยี Blockchain มาใช้ในงานบริการภาครัฐ โดยเฉพาะอย่างยิ่งเพื่อการจัดเก็บข้อมูลนั้นสามารถสร้าง



1

ความโปร่งใส Transparency

โดยการนำเทคโนโลยี Blockchain มาใช้ในการจัดเก็บข้อมูลภาครัฐ เป็นการเปิดโอกาสให้ประชาชน มีสิทธิเป็นเจ้าของข้อมูลของตนเองอย่างแท้จริง รวมไปถึงโอกาสในการเข้าถึงข้อมูลภาครัฐต่าง ๆ ได้ง่ายขึ้น ยกตัวอย่างเช่น ประเทศสหรัฐอเมริกาได้มีกฎหมายเสรีภาพด้านข้อมูลข่าวสาร (Freedom of Information Act: FOIA) โดยกำหนดให้หน่วยงานภาครัฐจะต้องเปิดเผยข้อมูลภาครัฐให้กับประชาชนตามที่มีการร้องขอโดยไม่รีรอ รวมไปถึงยุโรป



ก็มีกฎหมายในทำนองนี้ด้วยเช่นกัน แต่อย่างไรก็ดี ถึงแม้จะมีกฎหมายดังกล่าว แต่การบังคับใช้กฎหมายก็ยังไม่ค่อยมีประสิทธิภาพมากนัก ซึ่งโดยส่วนใหญ่



ข้อมูลที่ถูกร้องขอนั้นยังต้องใช้เจ้าหน้าที่รัฐในการพิจารณาว่าข้อมูลดังกล่าวควรเปิดเผยหรือไม่ รวมถึงการทำให้ข้อมูลดังกล่าวอยู่ในรูปแบบที่เหมาะสมต่อการเปิดเผย ดังนั้นเมื่อมีการร้องขอให้เปิดเผยข้อมูลตามกฎหมาย FOIA จึงทำให้เกิดความล่าช้าขึ้น ทั้งนี้การนำเทคโนโลยี Blockchain มาใช้เพื่อให้ประชาชนสามารถเข้าถึงข้อมูลภาครัฐได้



สามารถทำให้เกิดความโปร่งใส และเป็นการปฏิบัติตามกฎหมายว่าด้วย “เสรีภาพด้านข้อมูลข่าวสาร (FOIA)” โดยมีข้อแม้ว่าการเปิดให้ประชาชนสามารถเข้าถึงข้อมูลภาครัฐได้นั้นจะต้องไม่ละเมิดความเป็นส่วนตัว หรือไม่ละเมิดข้อมูลส่วนบุคคล โดยจะต้องมีการออกแบบระบบที่ดีเพื่อให้มั่นใจว่ามีการปกปิดตัวตน หรือข้อมูลต้องไม่สามารถระบุตัวตนได้ (Anonymous) อีกทั้งยังช่วยลดค่าใช้จ่ายของภาครัฐในการที่จะต้องบันทึก และจัดเก็บข้อมูลหลาย ๆ ครั้งสำหรับแต่ละหน่วยงาน โดยข้อมูลดังกล่าวสามารถถูกบันทึกอัตโนมัติโดยใช้ฟอร์มที่มีการออกแบบไว้ ซึ่งแบบฟอร์มดังกล่าวจะต้องมีการปกปิดหรือซ่อนข้อมูลที่มีความอ่อนไหวเอาไว้ ซึ่งในปี ค.ศ.2016 รัฐบาลประเทศอังกฤษ



ได้จัดทำรายงานขึ้นมาฉบับหนึ่งเกี่ยวกับการนำเทคโนโลยี Blockchain มาใช้ในการจัดเก็บข้อมูลภาครัฐ ยกตัวอย่างเช่น ข้อมูลเกี่ยวกับเงินบำนาญ (State Pensions) ข้อมูลความช่วยเหลือจากต่างประเทศ (Foreign Aid) ข้อมูลค่าใช้จ่ายทั่วไปของรัฐบาล (General Government Expenditure) โดยหน่วยงานภาครัฐสามารถเขียนข้อมูลเกี่ยวกับการใช้จ่ายต่าง ๆ ลงบน Ledger และ Ledger ดังกล่าวสามารถถูกกระจายไปยังทุกคนได้ ซึ่งจะช่วยให้เกิดความโปร่งใสและความรับผิดชอบเนื่องจากการหลอกลวง หรือการปลอมแปลงใด ๆ จะถูกตรวจสอบโดยประชาชนได้



2

การป้องกันการปลอมแปลง Tamper-Proof

การนำเทคโนโลยี Blockchain มาใช้ในการจัดเก็บข้อมูลภาครัฐสามารถช่วยสร้างความมั่นใจ และความน่าเชื่อถือให้กับข้อมูลหรือเอกสารที่ถูกบันทึกเข้าสู่ระบบ Blockchain แล้วจะไม่สามารถถูกเปลี่ยนแปลงหรือแก้ไขได้ ดังนั้นถึงแม้การนำเทคโนโลยี Blockchain มาใช้ใน





การจัดเก็บข้อมูลภาครัฐจะสามารถช่วยสร้างความโปร่งใส โดยการเปิดโอกาสให้ประชาชนมีสิทธิเป็นเจ้าของข้อมูลของตนเองอย่างแท้จริง รวมไปถึงโอกาสในการเข้าถึงข้อมูลภาครัฐต่าง ๆ ได้ง่ายขึ้น แต่อย่างไรก็ดีการจะนำเทคโนโลยี Blockchain มาใช้สำหรับการจัดเก็บข้อมูลภาครัฐนั้น นอกจากเรื่องของการสร้างความโปร่งใส และความปลอดภัยของข้อมูลแล้ว ยังจำเป็นต้องคำนึงถึงเรื่องของต้นทุน รวมถึงค่าใช้จ่ายสำหรับการบริหารจัดการ ควบคู่ไปกับเรื่องของความปลอดภัยร่วมด้วยในการตัดสินใจ



ข้อจำกัดของการนำเทคโนโลยี Blockchain มาใช้ในงานบริการภาครัฐ

ถึงแม้เทคโนโลยี Blockchain จะมีประโยชน์ในเรื่องของความปลอดภัยสูง และยากต่อการเปลี่ยนแปลงแก้ไขหากนำมาใช้ในการจัดเก็บข้อมูลภาครัฐ แต่ก็มีข้อควรระวังหากจะนำเทคโนโลยีดังกล่าวมาใช้ในการจัดเก็บข้อมูลภาครัฐดังต่อไปนี้

1

สิทธิส่วนบุคคล The Right to Privacy



การที่ข้อมูลใด ๆ เมื่อถูกบันทึกเข้าสู่ระบบ Blockchain แล้วจะไม่สามารถลบออกหรือแก้ไขได้ จึงอาจเป็นข้อจำกัดของการนำเทคโนโลยี Blockchain มาใช้งานเกี่ยวกับการจัดเก็บข้อมูลภาครัฐ (Government Record Keeping) ซึ่งเกี่ยวข้องกับสิทธิในความเป็นส่วนตัว (The Right to Privacy) โดยเฉพาะอย่างยิ่งเมื่อ EU ได้มีการออกกฎหมาย The General Data Protection Regulation: GDPR ว่าด้วยเรื่องสิทธิในการเป็นเจ้าของข้อมูล โดยประชาชนมีสิทธิร้องขอให้ลบข้อมูลของตนเองออกจากระบบใด ๆ ได้ (Right to be Forgotten) ดังนั้นการที่ไม่

สามารถลบข้อมูลที่ถูกบันทึกเข้าสู่ระบบ Blockchain ไปแล้วนั้น อาจจะเป็นได้ ทั้งข้อดีและข้อเสีย โดยข้อดีคือเหมาะแก่ การนำเทคโนโลยี Blockchain ไปใช้ใน เรื่องของการจัดเก็บข้อมูล (Record Keeping) สำหรับข้อมูลที่ต้องการ ความถูกต้องสูง และไม่ต้องการให้เกิด การเปลี่ยนแปลงแก้ไข เช่น ข้อมูลการ

ลงคะแนนเสียงเลือกตั้ง แต่หากนำไป จัดเก็บข้อมูลส่วนบุคคล โดยเฉพาะ ในยุโรปที่มีการใช้กฎหมาย GDPR ว่าด้วยเรื่องของสิทธิในการร้องขอให้ ลบข้อมูลของตนเองออกจากระบบได้ (Right to be Forgotten) จึงอาจเป็น ประเด็นที่ต้องพิจารณาต่อไป

2

ลิขสิทธิ์ Copyright

การนำเทคโนโลยี Blockchain ไปใช้ในการ จัดเก็บข้อมูลอาจจะมองได้ 2 มุม คือ ในมุมมองของเจ้าของลิขสิทธิ์ และผู้ละเมิด ลิขสิทธิ์ ซึ่งหากมีการเผยแพร่ข้อมูลที่ ละเมิดลิขสิทธิ์เข้าสู่ระบบ Blockchain แล้วจะไม่สามารถลบออกจากระบบได้ ดังนั้นจึงต้องมีความระมัดระวังใน การนำเทคโนโลยี Blockchain มาใช้ เพื่อจัดเก็บข้อมูลที่มีลิขสิทธิ์ นอกจาก ประเด็นดังกล่าวแล้วหากมีการ เผยแพร่ข้อมูลที่มีการละเมิดลิขสิทธิ์ เข้าสู่ระบบ Blockchain แล้วจะทำให้ เจ้าของลิขสิทธิ์ยากต่อการตรวจสอบ



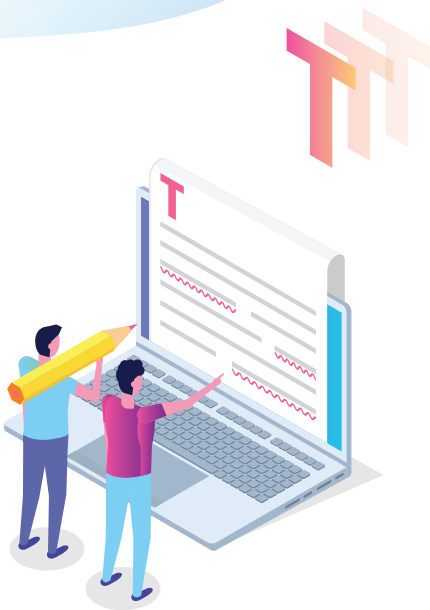
ผู้กระทำผิด เนื่องจากหลักการปกปิดตัวตน (Anonymous) ยกตัวอย่างเช่น ในยุโรป และสหรัฐอเมริกา ISP (Internet Service Provider) ส่วนใหญ่ พบกับปัญหา การนำเข้าสู่ข้อมูลที่มีการละเมิดลิขสิทธิ์ โดยผู้ใช้งานของตน ดังนั้นจึงได้มีการ ออกกฎหมายขึ้นมา 2 ฉบับ เพื่อคุ้มครอง ISP ดังนี้



The Digital Millennium Copyright Act (DMCA)



The Online Copyright Infringement Liability Limitation Act



ซึ่งเป็นเครื่องมือสำคัญในการขับเคลื่อนเกี่ยวกับการละเมิดลิขสิทธิ์ โดยกฎหมาย DMCA ได้ปกป้องสิทธิ์ของ ISP และ Webhost ต่าง ๆ ไว้ โดยมีการแจ้งเตือนเกี่ยวกับการละเมิดลิขสิทธิ์ หากมีการตรวจพบ ISP สามารถที่จะลบหรือระงับการเข้าถึงข้อมูล หรือสิ่งอื่นใดที่ได้รับการยืนยันว่ามีสิทธิ์ จึงเป็นประเด็นที่ต้องมีความระมัดระวังในการนำเทคโนโลยี Blockchain มาใช้เพื่อจัดเก็บข้อมูลที่มีลิขสิทธิ์ เนื่องจากหากมีการเผยแพร่ข้อมูลที่มีลิขสิทธิ์เข้าสู่ระบบ Blockchain จะไม่สามารถลบออกจากระบบได้ รวมถึงความยากต่อการตรวจสอบผู้กระทำผิดเนื่องจากหลักการปกปิดตัวตน (Anonymous) หากมีการเผยแพร่ข้อมูลที่มีการละเมิดลิขสิทธิ์เข้าสู่ระบบ Blockchain



3

การเซ็นเซอร์ข้อมูล Censorship

ประเด็นเกี่ยวกับการเซ็นเซอร์ข้อมูล โดยเฉพาะหน่วยงานภาครัฐที่ทำหน้าที่กำกับดูแลเรื่องต่าง ๆ รวมถึงการกระทำผิดกฎหมาย จะทำให้ตรวจสอบได้ยากขึ้นหากข้อมูลดังกล่าวถูกจัดเก็บโดยใช้เทคโนโลยี Blockchain ซึ่งอาจมีผลกระทบต่อหน่วยงานด้านความมั่นคง



จากข้อจำกัดดังกล่าวข้างต้น หน่วยงานภาครัฐของต่างประเทศ ส่วนใหญ่จึงนำ Private Blockchain มาใช้สำหรับการเก็บข้อมูล (Record Keeping) ของหน่วยงานภาครัฐมากกว่า Public Blockchain อีกทั้งด้วยข้อจำกัด ของ Public Blockchain ที่จำเป็นต้องใช้ Node จำนวนมากเพื่อทำหน้าที่ เป็น Miner ในการช่วย Validate Transaction จึงทำให้การประมาณ การต้นทุนที่แท้จริงในการลงทุน โดยเฉพาะด้าน Hardware นั้นเป็นไปได้ยาก แต่อย่างไรก็ดีค่าใช้จ่ายในการ Maintenance Blockchain โดยเฉพาะ อย่างยิ่ง Public Blockchain เช่น Bitcoin ถือได้ว่ามีต้นทุนสูง เมื่อเทียบกับระบบ แบบรวมศูนย์ (Centralized System) ที่ลงทุนเพียงแค่เครื่องเซิร์ฟเวอร์ และ เครื่องแบ็กอัพหรือเครื่องสำรองข้อมูล เท่านั้น แต่ใน Public Blockchain

นอกจากเรื่อง Hardware แล้ว ยังจำเป็นต้องมีการให้ผลตอบแทนกับ Miner ในการทำการตรวจสอบ (Validation) เพื่อให้ระบบ Blockchain นั้นสามารถ ดำเนินการต่อไปได้ อีกทั้งในการดำเนินการของระบบ Blockchain โดยเฉพาะ อย่างยิ่ง Public Blockchain จำเป็น ต้องใช้พลังงานอย่างมหาศาลเทียบเท่า กับการใช้พลังงานในเมืองที่มีประชากร 1.5 แสน ถึง 10 ล้านคน ขึ้นอยู่กับ ประสิทธิภาพของอุปกรณ์จัดเก็บข้อมูล และกระบวนการในการทำ Consensus รวมถึงการกระจาย Ledger แต่อย่างไร ก็ดีหากจะมีการนำ Private Blockchain มาใช้ในงานบริการภาครัฐนั้น หากสามารถ ควบคุมขนาดของเครือข่าย Blockchain ไม่ให้ใหญ่เท่า Public Blockchain ก็จะสามารถช่วยลดต้นทุนดังกล่าวลงได้ ถึงกระนั้นต้นทุนของการบริหารจัดการ และการลงทุนในเทคโนโลยี Blockchain ก็ยังมีมูลค่าสูงกว่าระบบแบบรวมศูนย์ (Centralized System) ที่ใช้ในปัจจุบัน อยู่ดี นอกจากนี้การเปลี่ยนแปลงข้อมูลที่ เคยจัดเก็บอยู่บนระบบเดิมขึ้นสู่ ระบบ Blockchain ยังต้องมีขนาดที่ เพียงพอเพื่อรองรับจำนวนประชากร ทั้งหมดได้ ซึ่งอาจจะต้องใช้เงินลงทุน





จำนวนมหาศาล ถึงแม้จะปรับมาใช้ Private Blockchain ที่อาจมีความน่าเชื่อถือน้อยกว่าแล้วก็ตาม

ดังนั้นการจะนำเทคโนโลยี Blockchain มาใช้เพื่อจัดเก็บข้อมูลภาครัฐ นอกจากเรื่องของการลงทุนที่สูงแล้ว อาจยังต้องคำนึงถึงประเด็นเกี่ยวกับความยากต่อการเปลี่ยนแปลงแก้ไขข้อมูลเมื่อถูกจัดเก็บเข้าสู่ระบบ Blockchain แล้ว โดยข้อมูลที่เหมาะสมกับการจัดเก็บโดยเทคโนโลยี Blockchain จึงไม่ควรเป็นข้อมูลที่ต้องมีการเปลี่ยนแปลงแก้ไขบ่อย ๆ แต่เหมาะกับข้อมูลที่ต้องการความปลอดภัยสูง ซึ่งหากพิจารณาใน

แง่ของการลงทุนและค่าใช้จ่ายในการบริหารจัดการระบบจัดเก็บข้อมูลแบบรวมศูนย์ (Centralized Database) อาจมีความสมเหตุสมผลมากกว่าในการจัดเก็บข้อมูลภาครัฐ แต่อย่างไรก็ตามหากพิจารณาในแง่ของความปลอดภัย การนำเทคโนโลยี Blockchain มาใช้สำหรับการจัดเก็บข้อมูลภาครัฐอาจมีความเหมาะสมมากกว่า ดังนั้นการจะนำเทคโนโลยี Blockchain มาใช้สำหรับการจัดเก็บข้อมูลภาครัฐจึงจำเป็นต้องคำนึงถึงเรื่องของต้นทุน รวมถึงค่าใช้จ่ายสำหรับการบริหารจัดการ ควบคู่ไปกับเรื่องของความปลอดภัยร่วมด้วยในการตัดสินใจ

รูปแบบการประยุกต์ใช้เทคโนโลยี Blockchain เพื่องานบริการภาครัฐ

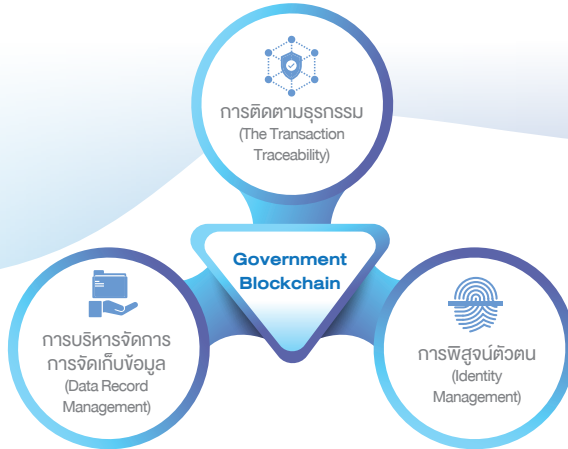
แนวคิดของรัฐบาลดิจิทัล คือ การนำเทคโนโลยีมาใช้เพื่อพัฒนาการบริหารจัดการภาครัฐ รวมถึงการให้บริการประชาชนที่ดีขึ้น แต่อย่างไรก็ดีการดำเนินการดังกล่าวนี้จะต้องมีความมั่นคงปลอดภัย โปร่งใส สามารถตรวจสอบได้ ดังนั้นด้วยคุณสมบัติของเทคโนโลยี Blockchain สามารถตอบสนองความต้องการดังกล่าวได้ ด้วยหลักการทำงานแบบ Distributed Ledger Technology และ Cryptography จึงทำให้มั่นใจได้ว่าข้อมูลที่ได้ถูกจัดเก็บด้วยเทคโนโลยี Blockchain นี้มีความมั่นคงปลอดภัย ไม่สามารถเปลี่ยนแปลงแก้ไขได้ ดังนั้นหน่วยงานภาครัฐของหลาย ๆ ประเทศจึงได้หันมาให้ความสนใจศึกษาถึงหลักการ และแนวทางการประยุกต์ใช้ จนนำไปสู่การนำเทคโนโลยี Blockchain มาใช้สำหรับงานบริการภาครัฐ อย่างเป็นรูปธรรมกันมากขึ้น ดังแสดงในตารางที่ 2



ตารางที่ 2: ตารางแสดงการประยุกต์ใช้เทคโนโลยี Blockchain สำหรับงานบริการภาครัฐในต่างประเทศ

Countries	Estonia	United State	China	India	Dubai: United Arab Emirates	Taiwan	Sweden	Australia	Gana	Georgia	Japan	Luxembourg	Malta	Norway	Switzerland	Ukraine	Republic of Georgia	Finland	Singapore	Peru
Blockchain Applications																				
Government Data Record Management																				
Asset Register (Land Registry, Vehicle Registry)	✓			✓	✓		✓		✓	✓	✓		✓			✓				
e-Voting	✓															✓				
Medical Record (e-Health)	✓	✓			✓								✓							
Digital Certificate (Birth Record, Education Certificate)	✓	✓																		
Identity Management																				
Individual Identity (e-Identity, Citizen I identification, eID)	✓	✓	✓	✓	✓	✓						✓			✓			✓		
Transaction Traceability																				
Supply Chain for Traceability (Food Safety, Pharmaceutical)			✓	✓	✓															
Tax Compliance and Custom for Fraud Traceability	✓			✓				✓											✓	✓

จากข้อมูลในตารางที่ 2 เป็นการสรุปตัวอย่างเพียงบางส่วนของ การนำเทคโนโลยี Blockchain มาใช้ในงานบริการภาครัฐของประเทศต่าง ๆ ซึ่งเมื่อทำการจัดกลุ่ม จะสามารถจำแนกออกเป็น 3 กลุ่มด้วยกันดังแสดงในรูปภาพที่ 16



รูปภาพที่ 16: การจัดกลุ่มการนำเทคโนโลยี Blockchain มาใช้กับงานบริการภาครัฐ

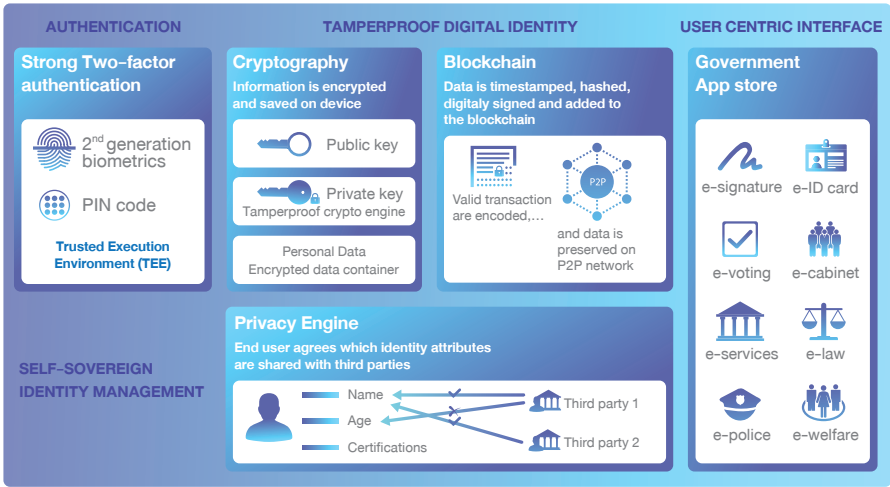


การพิสูจน์ตัวตน Identity Management

การยืนยันตัวตนบุคคลหรือการพิสูจน์ตัวตน (Identity Management) นั้น เป็นกระบวนการที่มีความเกี่ยวข้องกับชีวิตประจำวันในหลาย ๆ ด้านด้วยกัน ไม่ว่าจะเป็นการทำธุรกรรมกับทางธนาคาร การเข้ารับบริการ และสวัสดิการต่าง ๆ ของภาครัฐ รวมไปถึงการดำเนินการทางธุรกิจต่าง ๆ ซึ่งล้วนแล้วแต่ต้องมีความเกี่ยวข้องกับการยืนยันตัวตนหรือการพิสูจน์ตัวตนทั้งสิ้น ยิ่งในยุคปัจจุบันที่เป็นยุคของเทคโนโลยีด้วยแล้วนั้น การยืนยันตัวตนหรือการพิสูจน์ตัวตนนั้นยิ่งมีความสำคัญมากยิ่งขึ้น การยืนยันตัวตนหรือการพิสูจน์ตัวตนในปัจจุบันส่วนใหญ่ยังเป็น การใช้รหัสผ่าน (Password-Based Systems) เป็นหลัก อีกทั้งยังเป็นระบบที่ต้องอาศัยคนกลางคอยทำหน้าที่ในการบริหารจัดการ

ข้อมูลดังกล่าว โดยทำการจัดเก็บข้อมูลไว้ที่ศูนย์กลาง ซึ่งระบบดังกล่าวมีความเสี่ยงต่อการถูกโจมตีเข้าระบบเพื่อจารกรรมข้อมูลส่วนบุคคล (Identity Theft) และนำข้อมูลดังกล่าวไปขายให้กับอาชญากรเพื่อสวมรอยเป็นบุคคลนั้น ๆ หรือนำข้อมูลดังกล่าวไปใช้เพื่อกระทำความผิดอื่นใดได้ แต่ด้วยคุณสมบัติการทำงานและเทคโนโลยี Blockchain ซึ่งเป็นระบบแบบกระจายศูนย์ (Distributed Computing) และมีการจัดเก็บข้อมูลแบบ Shared Database ซึ่งถือว่าเป็นรูปแบบการบันทึกข้อมูลที่รับประกันความปลอดภัยว่าข้อมูลที่ถูกบันทึกไปก่อนหน้านี้ไม่สามารถที่จะเปลี่ยนแปลงหรือแก้ไขได้ โดยทุก ๆ ผู้ใช้งานจะเห็นข้อมูลชุดเดียวกันทั้งหมด จึงทำให้เกิดความสะดวกในการตรวจสอบ และบริหารจัดการการยืนยันตัวตนบุคคลหรือการพิสูจน์ อีกทั้งยังมีความปลอดภัยและมีประสิทธิภาพอีกด้วย

การทำงานของระบบยืนยันหรือพิสูจน์ตัวตนบนเทคโนโลยี Blockchain ดังแสดงในรูปภาพที่ 17 ใช้หลักการ “Self-Sovereign Identity” คือ การที่ประชาชนหรือองค์กรสามารถที่จะสร้างและจัดเก็บข้อมูลประจำตัวของตนไว้บนอุปกรณ์ของตนเองได้ โดยไม่ต้องมีคนกลางมาทำหน้าที่ในการจัดเก็บข้อมูลดังกล่าวอีกต่อไป ทำให้เกิดประสิทธิภาพในการตรวจสอบสำหรับผู้ที่ต้องการใช้ข้อมูลดังกล่าว อีกทั้งยังสามารถช่วยลดการใช้กระดาษลงได้โดยไม่จำเป็นต้องถ่ายเอกสารหลักฐานสำคัญเพื่อใช้ในการยืนยันตัวตน ยกตัวอย่างเช่น บัตรประชาชน สำเนาทะเบียนบ้าน สูติบัตร หรือเอกสารสำคัญทางราชการอีกต่อไป



รูปภาพที่ 17: ระบบยืนยันและพิสูจน์ตัวตนบนเทคโนโลยี Blockchain
 ที่มา: ปรับปรุงจาก (Parker, 2017)

กรณีศึกษาที่ 1

ระบบพิสูจน์และยืนยันตัวตนอิเล็กทรอนิกส์ Citizen Identification รัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา

รัฐอิลลินอยส์แห่งประเทศสหรัฐอเมริกาได้นำระบบ Identity Management บนเทคโนโลยี Blockchain มาใช้ในการเก็บสถิติบัตรของเด็กทารกแรกเกิด (Birth Registration) รวมถึงระบบพิสูจน์และยืนยันตัวตนอิเล็กทรอนิกส์ (Citizen Identification) โดยทางรัฐบาลได้ทำงานร่วมกับบริษัทสตาร์ทอัพ Evernym โดยแพทย์และผู้ปกครองของเด็กทารกเกิดใหม่สามารถลงทะเบียนสถิติบัตรบน



ระบบ Blockchain ซึ่งถูกออกแบบมาเพื่อใช้เป็นเครื่องมือในการเก็บข้อมูลของประชาชนในระยะยาว ทำให้รัฐบาลสามารถที่จะตรวจสอบข้อมูลเกี่ยวกับการเกิดของประชาชน รวมไปถึงข้อมูลทางชีวภาพ (Biometric) อื่น ๆ ได้ เช่น กรู๊ปเลือด ลายนิ้วมือ เสียง ม่านตา และดีเอ็นเอ โดยข้อมูลดังกล่าวจะถูกเข้ารหัสพร้อมทั้งใช้ลายเซ็นดิจิทัล (Digital Signature) เช่นกำกับและหลังจากนั้นข้อมูลก็จะถูกเก็บไว้ใน Distributed Ledger ที่สามารถเข้าถึงได้ เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น ซึ่งจะช่วยเพิ่มความน่าเชื่อถือให้กับระบบพิสูจน์ตัวตน และป้องกันการโจรกรรมเอกลักษณ์บุคคล (Identity Theft) ได้ โดยโครงการดังกล่าวจะเริ่มต้นจากการเก็บข้อมูลเด็กทารกแรกเกิด และเก็บข้อมูลทั้งหมดของประชาชนในลำดับถัดมา การนำระบบ Identity Management บนเทคโนโลยี Blockchain มาใช้ในการเก็บสูติบัตรของเด็กทารกแรกเกิด (Birth Registration) นั้น เป็นเพียงหนึ่งในหลาย ๆ โครงการของรัฐบาลรัฐอิสราเอลที่ต้องการพัฒนาระบบเทคโนโลยี Blockchain เพื่อนำมาใช้ในชีวิตประจำวันของประชาชนให้มากขึ้น

กรณีศึกษาที่ 2

ระบบการยืนยันตัวตนผู้ประสบภัย Refugees Identity Management องค์การสหประชาชาติ (The United Nation: UN)

นอกจากนี้ระบบ Identity Management บนเทคโนโลยี Blockchain ยังได้ถูกนำไปใช้เพื่อสนับสนุนภารกิจของ UN ซึ่งเป็นการร่วมมือระหว่างบริษัท Accenture และ Microsoft ในการสร้างระบบการยืนยันตัวตนโดยใช้วิธีตรวจสอบข้อมูลทางชีวภาพ (Biometric) ผ่านลายนิ้วมือและม่านตา โดย UN ได้เริ่มใช้งานระบบดังกล่าวกับผู้พลัดถิ่นในเอเชีย 29 ประเทศจำนวน 1.3 ล้านคน และจะขยายเป็น 7 ล้านคนในปี ค.ศ. 2020 รวมไปถึงโครงการอาหารโลก (World Food Program: WFP) แห่งสหประชาชาติ ยังได้นำระบบ Identity Management บนเทคโนโลยี Blockchain ไปใช้ในการยืนยันตัวตนของผู้พลัดถิ่น หรือผู้ประสบภัย เพื่อรับคุ้มครองแทนเงินสดสำหรับช่วยเหลือผู้พลัดถิ่น หรือประสบภัย โดยผู้รับคุ้มครองสามารถที่จะสแกนม่านตาของผู้ใช้คุ้มครอง ทำให้ทางเจ้าของร้านที่เข้าร่วมรายการสามารถแจกจ่ายอาหารให้กับทางผู้พลัดถิ่น ทั้งนี้การยกเลิกเงินสดแล้ว

หันมาใช้เทคโนโลยีดังกล่าวในการ
เยียวยาผู้อพยพหรือผู้ประสบภัยนั้น
จะช่วยอุดรอยรั่วทางการแจกจ่าย
อาหาร และทำให้อาหารเหล่านั้นถึงมือ
ผู้ประสบภัยได้อย่างครบถ้วน



การบริหารจัดการการจัดเก็บข้อมูล Data Record Management

หัวใจของการบริหารจัดการข้อมูลภาครัฐ คือ การบริหารจัดการความ
น่าเชื่อถือของข้อมูลที่เกี่ยวข้องกับ บุคคล องค์กร สิทธิพล และกิจกรรมต่าง ๆ
ของภาครัฐ นอกจากนี้ในการบริหารจัดการข้อมูลเหล่านี้ ไม่ว่าจะเป็นข้อมูล
การเกิด การตาย สถานภาพการสมรส การออกใบอนุญาตเกี่ยวกับการดำเนินธุรกิจ
และการโอนสิทธิพลต่าง ๆ รวมถึงข้อมูลเกี่ยวกับประวัติอาชญากรรม เป็นต้น
ล้วนแล้วแต่มีต้นทุน และความยุ่งยากในการบริหารจัดการรวมถึงการนำไป
ใช้งานทั้งสิ้น อีกทั้งข้อมูลบางอย่างยังไม่ถูกจัดเก็บอยู่ในรูปแบบอิเล็กทรอนิกส์
ซึ่งโดยส่วนใหญ่มักจะอยู่ในรูปแบบของแบบฟอร์มบนกระดาษ หากประชาชน
ต้องการเปลี่ยนแปลงหรือแก้ไขข้อมูลก็จำเป็นต้องไปดำเนินการด้วยตนเอง
ณ สถานที่ราชการที่เกี่ยวข้องนั้น ๆ แต่ด้วยคุณสมบัติของเทคโนโลยี Blockchain
ที่ใช้หลักการของ Distributed Ledger Technology (DLT) และ Cryptography
ซึ่งช่วยให้การเข้าถึง และการเข้าใช้ข้อมูลภาครัฐ รวมถึงการบริหารจัดการ
ความปลอดภัยและที่น่าเชื่อถือของข้อมูลภาครัฐทำได้ง่ายขึ้น ดังนั้นรัฐบาล
ในหลายประเทศจึงมีการนำเทคโนโลยี Blockchain มาใช้ในการจัดเก็บข้อมูล
ภาครัฐรวมถึงข้อมูลการลงทะเบียนเอกสารสำคัญที่ออกโดยหน่วยงานภาครัฐ
ยกตัวอย่าง เช่น

- ข้อมูลการลงคะแนนเสียงเลือกตั้ง (e-Voting)
- ข้อมูลประวัติการศึกษา (Educational Record)
- ข้อมูลประวัติการเกิด (Birth Record)
- ข้อมูลประวัติการรักษาพยาบาล (Medical Record)
- ข้อมูลการลงทะเบียนสินทรัพย์ต่าง ๆ (Asset Register)

กรณีศึกษาที่ 1

การจดทะเบียนที่ดิน Land Registry ประเทศอินเดีย

ประเทศอินเดียได้มีการนำเทคโนโลยี Blockchain มาใช้ในการจดทะเบียนที่ดิน (Land Registration) โดยที่ดินถือเป็นสินทรัพย์ที่มีมูลค่าสูง ซึ่งบ่อยครั้งมักเป็นสาเหตุของการเกิดกรณีพิพาท ปัญหาอาชญากรรม และการฉ้อโกง ดังนั้นการคุ้มครองสิทธิเหนือที่ดิน และการถือครองกรรมสิทธิ์ที่ดิน สำหรับผู้ซื้อจึงเป็นเรื่องสำคัญเนื่องจากประเด็นดังกล่าวถือเป็นปัจจัยพื้นฐานที่ส่งผลกระทบต่อความเชื่อมั่นด้านการลงทุนและการเติบโตทางเศรษฐกิจ ซึ่งปัญหากรณีพิพาทเรื่องที่ดินมักเป็นปัญหาที่เกิดขึ้นกับประเทศกำลังพัฒนาเป็นส่วนใหญ่ โดยเฉพาะประเทศอินเดีย

จึงได้นำเทคโนโลยี Blockchain มาใช้ในการจดทะเบียน/โอนกรรมสิทธิ์ โดยเฉพาะอย่างยิ่งสินทรัพย์ที่มีสภาพคล่องต่ำ ยกตัวอย่างเช่น ที่ดิน ซึ่งช่วยลดกระบวนการทางด้านเอกสารได้ อีกทั้งยังช่วยเพิ่มประสิทธิภาพกระบวนการทำธุรกรรมต่าง ๆ เกี่ยวกับอสังหาริมทรัพย์





กรณีศึกษาที่ 2

การจัดเก็บและส่งต่อข้อมูล ประวัติการรักษาพยาบาลของผู้ป่วย นครรัฐดูไบ ประเทศสหรัฐ อาหรับเอมิเรตส์

นครรัฐดูไบได้นำเทคโนโลยี Blockchain มาใช้ในการจัดเก็บและส่งต่อข้อมูลประวัติการรักษาพยาบาลของผู้ป่วยเพื่อให้ผู้ที่มีส่วนเกี่ยวข้องกับกระบวนการรักษาพยาบาลสามารถเข้าถึงข้อมูลได้อย่างปลอดภัย โดยนครรัฐดูไบซึ่งเป็นหุ้นส่วนกับ NMC Healthcare ในสหรัฐอาหรับเอมิเรตส์ (United Arab Emirates: UAE) ได้มองเห็นถึงความสำคัญดังกล่าว จึงได้ร่วมมือกับบริษัท Guardtime ซึ่งเป็นบริษัทผู้พัฒนาโซลูชันต่าง ๆ บนเทคโนโลยี

Blockchain สัญชาติเอสโตเนีย ในการนำระบบเวชระเบียนอิเล็กทรอนิกส์ (Electronic Health Records: EHR) บนเทคโนโลยี Blockchain มาใช้ ซึ่งการใช้งานระบบดังกล่าวช่วยให้ข้อมูลมีความถูกต้องปลอดภัย และเชื่อถือได้ตลอดกระบวนการที่เกิดขึ้นระหว่างผู้ให้บริการด้านสุขภาพและผู้ป่วย ทำให้มั่นใจได้ถึงความปลอดภัยของข้อมูลที่ได้รับ สำหรับผู้ป่วยที่มาปรึกษาแพทย์ของ NMC Healthcare ก็สามารถได้รับการบริการอย่างต่อเนื่องไม่ขาดตอน

นอกจากนี้การเริ่มต้นโครงการดังกล่าวของ NMC Healthcare สามารถช่วยเพิ่มประสิทธิภาพในการทำงานโดยการสร้างกระบวนการที่มีความปลอดภัยในการบันทึก จัดเก็บ และได้รับข้อมูลประวัติการรักษาของคนไข้ นอกจากการเพิ่มประสิทธิภาพของกระบวนการจัดเก็บข้อมูลดังกล่าวแล้วนั้น กระบวนการทำงานที่มีประสิทธิภาพยังสามารถช่วยเพิ่มประสิทธิภาพในการกำหนดแผนการและตารางนัดหมายของคนไข้ อีกทั้งยังง่ายต่อการเข้าถึงข้อมูลสุขภาพของทั้งคนไข้และบุคลากรทางการแพทย์อีกด้วย ซึ่งปัจจุบันประวัติการรักษาคนไข้ต่าง ๆ นั้นมักจะอยู่ในรูปแบบของ



กระดาษเป็นหลัก เช่น ผลการตรวจเลือด ผล X-Ray และอื่น ๆ อีกทั้งโรงพยาบาลส่วนใหญ่ก็ไม่ได้มีการแชร์ข้อมูลดังกล่าวร่วมกัน ดังนั้นการนำเทคโนโลยี Blockchain มาใช้ในการจัดเก็บข้อมูล ประวัติการรักษาของคนไข้ทำให้สามารถแชร์ข้อมูลดังกล่าวระหว่างโรงพยาบาลได้ อีกทั้งยังสามารถเชื่อมั่นได้ถึงความปลอดภัย และปลอดภัยของข้อมูล ด้วยเทคโนโลยี Blockchain ที่มีรูปแบบของการบันทึกข้อมูลที่รับประกันความปลอดภัยว่าข้อมูลที่ถูกบันทึกไปก่อนหน้านี้ไม่สามารถที่จะเปลี่ยนแปลงหรือแก้ไข โดยทุก ๆ ผู้ใช้งานจะเห็นข้อมูลชุดเดียวกันทั้งหมด การทำงานของ Blockchain ใช้หลักการ Cryptography และความสามารถของ Distributed

Computing เพื่อสร้างกลไกความน่าเชื่อถือสำหรับการแชร์ข้อมูลเวชระเบียนของผู้ป่วยระหว่างหน่วยงานให้บริการด้านสุขภาพ ซึ่งข้อมูลเวชระเบียนของผู้ป่วยนั้นถือเป็นข้อมูลที่มีความละเอียดอ่อน นอกจากนี้การนำเทคโนโลยีดังกล่าวมาใช้งานนั้นจะช่วยให้คนไข้สามารถเข้ารับการรักษาได้ในทุก ๆ คลินิกและโรงพยาบาล โดยคนไข้สามารถมั่นใจได้ว่าทุก ๆ สถานพยาบาลนั้นจะมีข้อมูลประวัติการรักษาของคนไข้รายนั้น ๆ แล้ว ถึงแม้จะไม่เคยได้รับการรักษาในสถานพยาบาลดังกล่าวมาก่อน ซึ่งในกรณีเร่งด่วนฉุกเฉินข้อมูลดังกล่าวจะมีประโยชน์ต่อการรักษาของคนไข้เป็นอย่างมาก และอาจสามารถช่วยรักษาชีวิตของคนไข้เอาไว้ได้

กรณีศึกษาที่ 3:

การออกใบ Certificate ให้กับเพชร นครรัฐดูไบ ประเทศสหรัฐอาหรับเอมิเรตส์

นครรัฐดูไบได้นำเทคโนโลยี Blockchain มาใช้ในการออกใบ Certificate ให้กับเพชร โดย The Dubai Multi Commodities Centre ได้นำเทคโนโลยี Blockchain เข้ามาใช้ในการออกใบ Certificate ให้กับเพชร หรือที่รู้จักกันในชื่อ “Kimberley Certificates”⁵ เพื่อเป็นการลดปัญหา

ข้อขัดแย้งเกี่ยวกับเพชร โดยกระบวนการ คิมเบอร์ลีย์ คือ การให้รัฐบาลของแต่ละ ประเทศรับรองว่า เพชรส่งออกมาได้มาจากเหมืองและธุรกิจที่ถูกกฎหมาย และผู้ประกอบการที่มีใบรับรองเท่านั้น จึงจะสามารถนำเพชรเข้าสู่ตลาดโลกได้ เนื่องจากใบรับรองนี้จะมีรายละเอียด ของทุกขั้นตอนในการผลิตเพชร ตั้งแต่



นอกจากเหมืองถึงผู้ค้าปลีก ประเทศ
ที่ตกลงร่วมใน Kimberley Process
จะไม่ได้รับอนุญาตให้ค้าขายกับประเทศ
อื่นที่ไม่ใช่สมาชิก จึงเป็นที่เชื่อกันว่า
โครงการนี้มีส่วนช่วยลดการรั่วไหลของ
เพชรแห่งความขัดแย้งเข้าสู่ตลาดอัญมณี
โลกได้อย่างมาก

ทั้งนี้นครรัฐดูไบได้ชื่อว่าเป็น “City
of Gold” หรือเมืองแห่งทองคำ ดังนั้น
การส่งเสริมการค้าขาย การส่งออกและ
นำเข้าทองคำรวมไปถึงอัญมณีอื่น ๆ
จึงเป็นเรื่องสำคัญจนกระทั่งต้องตั้ง
เขตธุรกิจเสรีเพื่อการนี้โดยเฉพาะ สินค้า

ประเภททองคำ เพชร พลอยสีต่าง ๆ
และโลหะมีค่าประเภททองคำขาว
พัลลาเดียม เงิน เป็นสินค้าที่มีการส่งออก
และนำเข้าจากทวีปต่าง ๆ โดยมีนครรัฐ
ดูไบเป็นศูนย์กลาง ดังนั้น The Dubai
Multi Commodities Centre จึงได้
นำเทคโนโลยี Blockchain เข้ามาใช้
ในการออก “Kimberley Certificates”
เพื่อเป็นการลดปัญหาการซื้อขัดแย้ง
เกี่ยวกับเพชร อีกทั้งยังสามารถตรวจสอบ
รายละเอียดของทุกขั้นตอนในการผลิต
เพชร ตั้งแต่ออกจากเหมืองถึงผู้ค้า
ปลีกได้



⁵ Kimberley Certificates คือ การรับรองเพชรตามกระบวนการคิมเบอร์ลีย์เพื่อป้องกันไม่ให้
เพชรแห่งความขัดแย้ง (Conflict Diamond) หรือที่รู้จักกันในชื่อเพชรสีเลือด (Blood Diamond)
ซึ่งเป็นเพชรที่ได้จากเหมืองในพื้นที่ที่ถูกควบคุมโดยกลุ่มกบฏในประเทศเซียร์รา ลีโอน ซึ่งต่อต้าน
รัฐบาลที่ได้รับการยอมรับจากนานาชาติ กลุ่มกบฏขายเพชรนี้เพื่อได้เงินเป็นทุนซื้ออาวุธและ
เสริมสร้างให้กองทัพแข็งแกร่งยิ่งขึ้น

กรณีศึกษาที่ 4

การลงคะแนนเสียงเลือกตั้ง i-Voting ประเทศเอสโตเนีย

ประเทศเอสโตเนียได้นำเทคโนโลยี Blockchain มาใช้กับการลงคะแนนเสียงเลือกตั้ง หรือที่รู้จักกันในชื่อ i-Voting นั่นเอง โดยประเทศเอสโตเนียมีการใช้ระบบการลงคะแนนแบบดิจิทัล (Digital Voting) ตั้งแต่ปี ค.ศ. 2005 และอนุญาตให้มีการลงคะแนนเสียงผ่านระบบออนไลน์ในปี ค.ศ. 2007 ต่อมาในปี ค.ศ. 2015 จึงได้มีการนำระบบการลงคะแนนเสียงที่ทำงานอยู่บนเทคโนโลยี Blockchain โดยหลักการพื้นฐานของระบบ i-Voting ก็คือบัตรประชาชนในรูปแบบดิจิทัล (Digital ID Card) ซึ่งประชาชนทุกคนในประเทศเอสโตเนียจะต้องมี โดยในบัตรประชาชนจะบรรจุข้อมูลที่ใช้สำหรับยืนยันตัวตนบุคคล โดยข้อมูลดังกล่าวจะถูกเข้ารหัสไว้เพื่อใช้ในการทำธุรกรรมออนไลน์ต่าง ๆ รวมไปถึงการลงคะแนนเสียงผ่านระบบ i-Voting ซึ่งเทคโนโลยี Blockchain จะถูกนำมาใช้ในขั้นตอนของการนำส่งบัตรลงคะแนน โดยทุก ๆ บัตรลงคะแนน หลังจากได้รับการตรวจความถูกต้องตามกระบวนการต่าง ๆ แล้ว จะต้องมีการ



ประทับเวลา (Time Stamp) และข้อมูลดังกล่าวจะถูกจัดเก็บบนระบบ Blockchain เพื่อทำหน้าที่พิสูจน์การมีอยู่จริงของบัตรลงคะแนนนั้น ๆ หรือที่เรียกว่า Proof of Existence คือการพิสูจน์การมีอยู่จริงของเอกสารต่าง ๆ

ประโยชน์ของการนำเทคโนโลยี Blockchain มาใช้กับการลงคะแนนเสียงเป็นอีกทางเลือกในการแก้ปัญหาการทุจริตการเลือกตั้ง จากการลงคะแนนด้วยกระดาษซึ่งมีช่องโหว่มากมายที่จะทำให้เกิดการทุจริต แต่การใช้เทคโนโลยี Blockchain ในการลงคะแนนเสียงสามารถช่วยลดโอกาสในการทุจริตลงได้ ทำให้การเลือกตั้งมีความเป็นธรรมมากขึ้น โดยอย่างยิ่งในการนับคะแนน เนื่องจากไม่สามารถทำการทุจริตในการเลือกตั้งได้โดยไม่ทิ้งร่องรอยไว้ภายใต้

ระบบ Blockchain อีกทั้งยังช่วยทำให้การเลือกตั้งมีความสะดวกมากขึ้น และสามารถเข้าถึงผู้มีสิทธิลงคะแนนเสียงได้มากขึ้นจึงเป็นการส่งเสริมกระบวนการประชาธิปไตยอีกทางหนึ่ง นอกจากนี้ในแง่ความปลอดภัยและความเป็นส่วนตัวของข้อมูล เทคโนโลยี Blockchain สามารถออกแบบการเข้ารหัสเพื่อปกปิดตัวตนรักษาความเป็นส่วนตัวและข้อมูลการมีส่วนร่วมทางการเมืองได้อีกด้วย ดังนั้นเทคโนโลยี Blockchain จึงกลายเป็นเทคโนโลยีสำคัญที่จะทำให้เกิดความโปร่งใสในการลงคะแนนเสียงได้มากขึ้น



การติดตามธุรกรรม Transaction Traceability

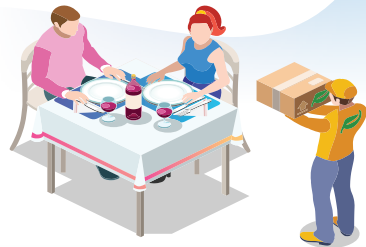
การนำเทคโนโลยี Blockchain มาใช้กับการตรวจสอบติดตามธุรกรรมแบบย้อนกลับทั้งห่วงโซ่อุปทาน (Supply Chain Transaction Traceability) ซึ่งสามารถช่วยในเรื่องเกี่ยวกับการบริหารจัดการข้อมูลให้กับสมาชิกที่มีความเกี่ยวข้องทั้งห่วงโซ่อุปทาน เพื่อให้เกิดความโปร่งใส (Transparency) ความเป็นกลาง (Neutrality) ความน่าเชื่อถือ (Reliability) และความมั่นคงปลอดภัยของข้อมูล (Security) โดยการกระจายข้อมูลที่มีความน่าเชื่อถือ และตรวจสอบได้ให้กับทุกคนที่มีความเกี่ยวข้องทั้งห่วงโซ่อุปทาน ซึ่งแต่เดิมจะต้องอาศัยคนกลางที่ได้รับความเชื่อถือจากทุกฝ่าย คอยเป็นคนบริหารจัดการข้อมูลดังกล่าว โดยระบบการบริหารจัดการข้อมูลแบบรวมศูนย์ (Centralized System) ดังกล่าวนั้นง่ายต่อการถูกปลอมแปลงและทุจริตโดยเจ้าหน้าที่ผู้ดูแลระบบ หากมีการติดสินบนเจ้าหน้าที่ดังกล่าว เนื่องจากให้อำนาจคนกลางในการบริหารจัดการข้อมูล รวมถึงการถูกเจาะระบบ (Hacking) ซึ่งจะทำให้ข้อมูลในระบบไม่สามารถเชื่อถือได้อีกต่อไป ดังนั้นในปัจจุบันหน่วยงานภาครัฐในหลาย ๆ ประเทศจึงได้ให้ความสนใจและนำเทคโนโลยี Blockchain มาใช้กับการตรวจสอบติดตามธุรกรรมแบบย้อนกลับทั้งห่วงโซ่อุปทาน (Supply Chain Transaction Traceability) ในหลาย ๆ กรณีด้วยกัน

กรณีศึกษาที่ 1

Food Safety Traceability Us: เกาหลี

การนำเทคโนโลยี Blockchain มาใช้กับการตรวจสอบความปลอดภัยของอาหารทั้งห่วงโซ่อุปทาน (Food Supply Chain Traceability System) โดยในยุคปัจจุบันความปลอดภัยด้านอาหาร (Food Safety) กำลังเป็นประเด็นที่ได้รับความสนใจทั้งในแวดวงวิชาการ ภาคธุรกิจ รวมไปถึงภาครัฐ โดยเฉพาะอย่างยิ่งความปลอดภัยด้านอาหาร ถูกจัดอยู่ในแผนเป้าหมายการพัฒนาอย่างยั่งยืน (Sustainable Development Goal: SDG) ซึ่งถูกพัฒนาโดยองค์การสหประชาชาติ (The United Nation) ดังนั้นในทุก ๆ ภาคส่วนจึงได้มีความพยายามในการคิดค้น และพัฒนานวัตกรรมเพื่อตรวจสอบความปลอดภัยของอาหาร (Food Safety Traceability)

บวกกับวิวัฒนาการของ IoT (Internet of Things) และเทคโนโลยี Blockchain ทำให้สามารถตรวจสอบความปลอดภัยของอาหารได้ตั้งแต่กระบวนการผลิตจนถึงมือผู้บริโภคได้ อีกทั้งยังสามารถทำการตรวจสอบได้แบบ Real Time และเป็นไปตามมาตรฐาน HACCP⁶ (Hazard Analysis and Critical Control Points) ยกตัวอย่างเช่น การปนเปื้อนสารพิษในนมผง อันเนื่องมาจากระบบแบบรวมศูนย์ (Centralized System) ที่เอื้อให้เกิดการทุจริต (Corruption) และการถูกโจมตีโดยแฮกเกอร์ (Hacking)



⁶ ระบบ HACCP คือ การวิเคราะห์อันตราย และจุดวิกฤติที่ต้องควบคุม หรือระบบ HACCP คือ ระบบการจัดการคุณภาพด้านความปลอดภัย ซึ่งใช้ในการควบคุมกระบวนการผลิตให้ได้ อาหารที่ปราศจากอันตรายจากเชื้อจุลินทรีย์ สารเคมี และสิ่งแปลกปลอมต่าง ๆ โดยถือเป็นมาตรฐานสากลตามข้อกำหนดของคณะกรรมการโครงการมาตรฐานอาหาร FAO/ WHO (Codex Alimentarius Commission) ที่ประเทศต่าง ๆ สามารถนำไปเป็นแนวทางในการประยุกต์ใช้เพื่อสร้างความมั่นใจในอุตสาหกรรมอาหารทั้งโดยผู้ผลิต และผู้บริโภค ซึ่งถูกกำหนดโดย NASA ในปี 1960s



กรณีศึกษาที่ 2

Pharmaceutical Supply Chain Traceability ประเทศไทย

ประเทศไทยได้นำเทคโนโลยี Blockchain มาใช้ในการทำ Supply Chain Traceability ในอุตสาหกรรมยา ในการติดตามค้นหาการรักษาโรค ซึ่งทำให้ผู้ที่เกี่ยวข้องในห่วงโซ่อุปทานยา (Pharmaceutical Supply Chain) สามารถเข้าถึงข้อมูลได้ง่ายขึ้น และแจ้งเตือน

เมื่อมีการปลอมแปลงยา เนื่องจากข้อมูลได้รับการพิสูจน์ทราบตามเอกสารต่าง ๆ จึงทำให้สามารถระบุที่มาของยาแต่ละชนิดว่ามาจากโรงงานใด และเป็นไปตามที่ระบุเอาไว้หรือไม่นั่นเอง เพื่อป้องกันการปลอมแปลงข้อมูล ทำให้เกิดความโปร่งใสและเชื่อถือได้

กรณีศึกษาที่ 3:

Industrial Hemp Supply Chain Traceability รัฐโคโลราโด แห่งประเทศสหรัฐอเมริกา

รัฐโคโลราโดแห่งประเทศสหรัฐอเมริกาได้ร่วมมือกับ The Institute of Cannabis Research at Colorado State University - Pueblo (Institute) ในการพัฒนาระบบตรวจสอบเส้นทางการซื้อขายกัญชารวมไปถึงผลิตภัณฑ์แปรรูปต่าง ๆ ในอุตสาหกรรมกัญชา (Industrial Hemp) ตั้งแต่ผู้ผลิตไปจนถึงผู้ซื้อและผู้ขาย โดยใช้เทคโนโลยี Blockchain รวมไปถึงการออกใบอนุญาตในการดำเนินธุรกิจเกี่ยวกับกัญชา ทั้งนี้การซื้อขายกัญชาจะต้องเป็นการซื้อขายจากผู้ที่ได้รับใบอนุญาตในการดำเนินธุรกิจเกี่ยวกับกัญชาเท่านั้น ซึ่งการนำเทคโนโลยี



Blockchain มาใช้ในอุตสาหกรรมกัญชานั้นช่วยให้รัฐโคโลราโดสามารถบังคับใช้กฎหมาย และการจัดเก็บรายได้จากการทำอุตสาหกรรมกัญชาได้อย่างมีประสิทธิภาพยิ่งขึ้น รวมไปถึงสามารถช่วยตรวจสอบการกระทำความผิดอันเนื่องมาจากการซื้อขายกัญชาที่ผิดกฎหมายจากผู้ที่ไม่ได้รับอนุญาต นอกจากนี้รัฐโคโลราโดได้มีการออกกฎหมายที่สำคัญว่าด้วยเรื่องการนำเทคโนโลยี Blockchain มาใช้ในการตรวจสอบการกระทำความผิดเกี่ยวกับอุตสาหกรรมกัญชา รวมไปถึงผลิตภัณฑ์ต่าง ๆ ที่มีส่วนผสมของกัญชาตั้งแต่กระบวนการผลิตไปจนถึงกระบวนการซื้อขาย





กรณีศึกษาที่ 4:

Tax Compliance for EU-Cross Broader Trade to Prevent Fraud and Detection สหภาพยุโรป (European Union: EU)

นอกจากการนำเทคโนโลยี Blockchain เข้ามาใช้ในการตรวจสอบย้อนกลับของการทำธุรกรรมต่าง ๆ แล้วยังได้มีการประยุกต์ใช้การตรวจสอบย้อนกลับของการทำธุรกรรมในเรื่องของภาษี ยกตัวอย่างเช่น สหภาพยุโรป (European Union: EU) ได้นำเทคโนโลยี Blockchain มาใช้ในการตรวจสอบเรื่องระบบภาษี ในการทำ Tax Refund สำหรับการค้าขายระหว่างประเทศสมาชิก EU ด้วยกัน (Tax Compliance for EU-Cross Broader Trade to Prevent Fraud and Detection) โดยสาระสำคัญ

ของระบบดังกล่าวคือ การติดตามธุรกรรมการซื้อขาย ตั้งแต่โรงงานผลิตไปจนถึงผู้ซื้อ โดยมั่นใจได้ว่าทุก ๆ ธุรกรรม จะไม่สามารถเปลี่ยนแปลงและแก้ไขได้ รวมไปถึงเอกสารใบวางบิลหรือใบแจ้งหนี้ (Invoice) ซึ่งถือเป็นหลักฐานสำคัญในการขอทำ Tax Refund เมื่อมีการซื้อขายหรือนำเข้าสินค้าระหว่างประเทศสมาชิก EU ด้วยกัน ดังนั้นด้วยคุณสมบัติของเทคโนโลยี Blockchain ในเรื่องของความยากต่อการเปลี่ยนแปลง (Immutability) จึงได้ถูกนำมาใช้ในการตรวจสอบย้อนกลับของการทำธุรกรรม เพื่อป้องกันการทุจริตในรูปแบบต่าง ๆ

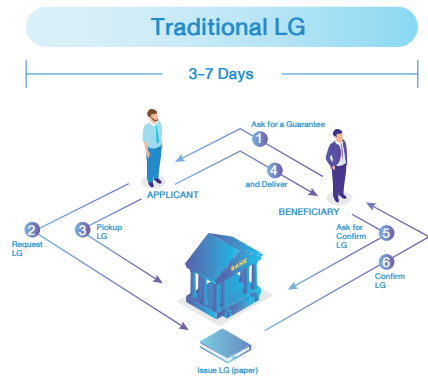
กรณีศึกษาที่ 5:

Letter of Guarantee on Blockchain : e-LG on Blockchain ประเทศไทย

การนำเทคโนโลยี Blockchain มาใช้ในการออกหนังสือค้ำประกัน (Letter of Guarantee) หรือตัวย่อ LG โดยปัจจุบันธนาคารมีหน้าที่ให้บริการออกหนังสือค้ำประกันให้แก่บริษัทลูกค้า ที่ประสงค์จะยื่นประมุลงาน หรือติดต่อทำสัญญากับหน่วยงานราชการ หรือบริษัทผู้รับผลประโยชน์ โดยนำหนังสือค้ำประกันของธนาคารไปวางเป็นประกันแทนการวางหลักประกันแทนหลักทรัพย์อื่น ๆ เช่น เงินสด พันธบัตรที่ดิน เพื่อใช้เป็นหลักประกันในการค้าประกันสัญญาหรือข้อตกลง เพื่อรับรองว่าหากคู่สัญญาไม่ปฏิบัติตามเงื่อนไขสัญญา ธนาคารจะเป็นผู้รับผิดชอบตามสัญญาค้ำประกัน

โดยในการขอออกหนังสือค้ำประกันแบบกระดาษรูปแบบเดิม มีระยะเวลาที่ใช้ในการออกหนังสือค้ำประกันตั้งแต่นับขอหนังสือค้ำประกันไปยังการตรวจสอบจากผู้รับผลประโยชน์ใช้เวลาประมาณ 3-7 วัน โดยเวลาส่วนใหญ่จะใช้ไปกับการ

รับส่งหนังสือให้กับผู้ที่เกี่ยวข้องต่าง ๆ การสอบถามสถานะการออกหนังสือ การตรวจสอบความถูกต้องของหนังสือ อีกทั้งมีต้นทุนในการจัดเก็บเอกสาร เนื่องจากเป็นหนังสือสำคัญที่ต้องทำการจัดเก็บไปตลอดอายุสัญญาเพื่อใช้ในกรณีมีการฟ้องร้อง โดยเฉพาะหน่วยงานรัฐและองค์กรขนาดใหญ่ที่มีการทำสัญญาเป็นจำนวนมาก ต้องมีการสร้างห้องจัดเก็บเอกสาร ซึ่งการคั้นหานั้นใช้เวลานานจากจำนวนปริมาณ ส่งผลให้มีต้นทุนทั้งในด้านการลงทุนและการดูแลรักษา



รูปภาพที่ 18: ภาพขั้นตอน และกระบวนการของการขอออกหนังสือค้ำประกันแบบกระดาษรูปแบบเดิม

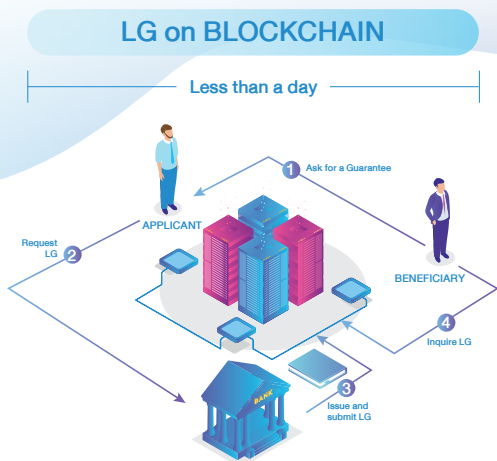
จากปัญหาดังกล่าว บริษัท บีซีไอ (ประเทศไทย) หรือ BCI ที่เกิดจากความร่วมมือของธนาคาร รัฐบาล และองค์กรธุรกิจชั้นนำ หลายแห่งภายใต้โครงการ Thailand Blockchain Community Initiative ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทย ได้เปิดให้บริการหนังสือค้ำประกันอิเล็กทรอนิกส์ผ่านระบบบล็อกเชน (Letter of Guarantee on Blockchain : e-LG on Blockchain) โดยได้เริ่มให้บริการจริงตั้งแต่เดือนมิถุนายน 2562 ที่ผ่านมา ซึ่งได้รับการพัฒนาขึ้นเพื่อแก้ปัญหา (Pain point) ให้กับผู้ใช้งานที่เกี่ยวข้องทุกส่วน ดังนี้

1. ช่วยลดระยะเวลาในการออกหนังสือค้ำประกัน
2. ใช้งานผ่านอิเล็กทรอนิกส์ 100% ทำให้ลดการใช้กระดาษ และต้นทุนในการจัดเก็บเอกสาร
3. เพิ่มความน่าเชื่อถือของเอกสาร และลดกระบวนการตรวจสอบ
4. สร้างมาตรฐานเดียวของหนังสือค้ำประกันกับทุกธนาคาร
5. ลดขั้นตอนการกรอกข้อมูลจากกระดาษเข้าระบบ และความผิดพลาดที่อาจเกิดจากมนุษย์
6. สามารถค้นหาเอกสารได้อย่างสะดวกและรวดเร็ว



รูปภาพที่ 19: ภาพการเปิดตัว บีซีไอ ณ ธนาคารแห่งประเทศไทย

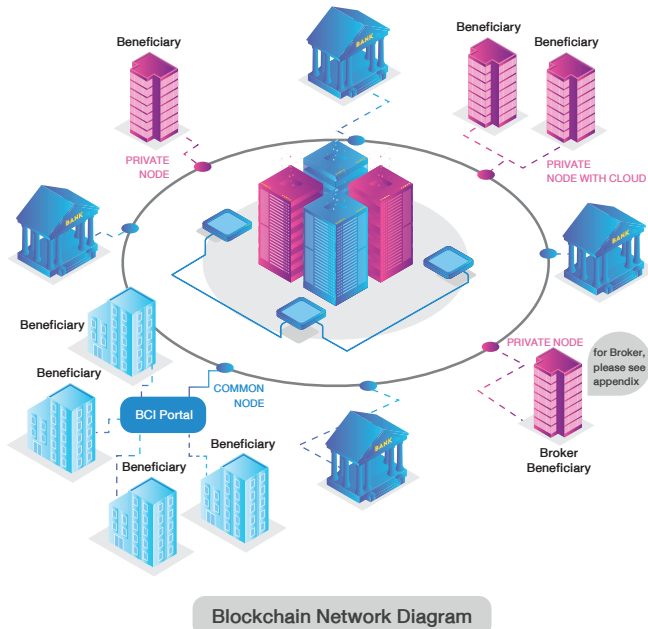
ด้วยเทคโนโลยี Blockchain จะช่วยลดระยะเวลาในการออกหนังสือค้ำประกันเหลือเพียง ไม่เกิน 1 วัน ข้อมูลต่าง ๆ จะถูกจัดเก็บไว้บนคลาวด์โดยสามารถบริหารและกำหนดสิทธิการเข้าถึงได้ ทำให้ข้อมูลถูกจัดเก็บอย่างปลอดภัยบนระบบ ช่วยลดขั้นตอนการนำส่งเอกสารกระดาษ และช่วยลดเวลาในการตรวจสอบที่มาของเอกสาร เพราะผู้ให้บริการสามารถมั่นใจได้ว่าเอกสารดังกล่าวออกจากธนาคารจริง



รูปที่ 20: ภาพขั้นตอนและกระบวนการของการขอออกหนังสือค้ำประกันอิเล็กทรอนิกส์ผ่านระบบบล็อกเชน

ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทย บริการ e-LG on Blockchain ดังกล่าวได้ผ่านมาตรฐานในระดับเดียวกับกับภาคธนาคาร เช่น มีการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management and Penetration Testing) ทดสอบประสิทธิภาพ (performance test) มีการทดสอบใน Regulatory Sandbox ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทย เพื่อให้ผู้ใช้บริการมั่นใจได้ว่า ระบบมีการดูแลรักษาความปลอดภัยของระบบงานและข้อมูล มีความถูกต้องเชื่อถือได้ สามารถใช้งานได้อย่างต่อเนื่อง มีการรักษาความปลอดภัยด้านไซเบอร์ และมีการรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคลของลูกค้า โดยมีกำหนดการออกจาก Regulatory Sandbox ภายในต้นปี พ.ศ.2564 นี้

ในปัจจุบันบริการหนึ่งสื่อค้าประกันอิเล็กทรอนิกส์ผ่านระบบบล็อกเชน ให้กับกลุ่มธนาคารพาณิชย์ และกลุ่มบริษัทเอกชน โดยมีผู้เข้าใช้บริการ แล้วทั้งสิ้นจำนวน 17 ธนาคาร และมีหน่วยงานรัฐวิสาหกิจ รวมถึงบริษัท ขนาดใหญ่ในภาคธุรกิจเข้าร่วมใช้บริการจำนวน 10 บริษัทฯ



รูปที่ 21: รูปแสดงโครงสร้างโดเมนของเน็ตเวิร์คบล็อกเชนและเชื่อมต่อ

ในส่วนของที่เกี่ยวข้อกับหน่วยงานภาครัฐปัจจุบันทาง BCI ได้มีความร่วมมือกับกรมบัญชีกลางซึ่งเป็นศูนย์กลางการปฏิบัติงานด้านการจัดซื้อจัดจ้างสำหรับภาครัฐและเอกชน พัฒนาระบบให้บริการหนังสือค่าประกันอิเล็กทรอนิกส์หรือ e-LG ผ่านเทคโนโลยีบล็อกเชน สำหรับการจัดซื้อจัดจ้างภาครัฐบนระบบอิเล็กทรอนิกส์บนระบบ e-GP ซึ่งนับเป็นครั้งแรกของหน่วยงานราชการที่เปิดให้มีการใช้ e-LG ทำให้การยื่นหนังสือรับรองกับภาครัฐมีความสะดวกมากขึ้น สามารถอนุมัติรายการได้เร็วสุดภายใน 10 นาที จากเดิมที่ต้องใช้เวลากว่า 3-7 วัน ให้บริการด้านการจัดซื้อจัดจ้างภาครัฐมีความโปร่งใส เป็นธรรม ภายใต

มาตรฐานความปลอดภัย ที่ได้รับการยอมรับในระดับสากล ลดการใช้กระดาษ ลดการคายก๊าซคาร์บอน (Carbon Footprint) เพื่อสร้างสิ่งแวดล้อมที่ดี ลดความทับซ้อนของการเชื่อมต่อกับธนาคารต่าง ๆ เดิม กรมบัญชีกลางเชื่อมต่อกับธนาคารในรูปแบบ Host2Host ส่งผลให้ต้องพัฒนาการเชื่อมต่อไปยังทุกธนาคาร กรณีมีการเปลี่ยนแปลงเกิดขึ้น เช่นกรมบัญชีกลางต้องการแก้ไขข้อมูลในฟิลด์ โดยต้องทำการแก้ไขทุกการเชื่อมต่อ แต่เมื่ออยู่บนระบบ e-LG การเชื่อมต่อเหลือเพียงแค่ระบบเดียวคือเชื่อมกับระบบ Blockchain ที่มีธนาคารต่าง ๆ ร่วมอยู่แล้ว ทำให้แก้ไขเพียงแค่ครั้งเดียวก็สามารถรองรับกับทุกธนาคารได้





รูปภาพที่ 22: ภาพการเปิดตัวบริการหนังสือค้ำประกันอิเล็กทรอนิกส์ ระบบ e-GP ผ่านเทคโนโลยีบล็อกเชน

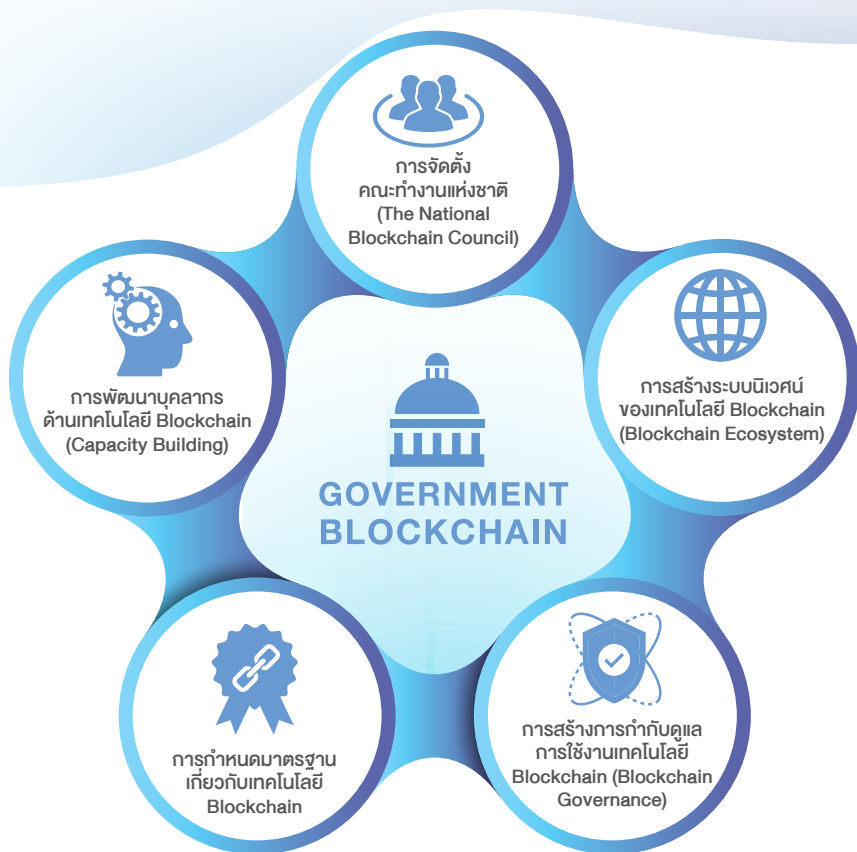
จากปัจจุบันมีการใช้หนังสือค้ำประกันอยู่ 500,000 ฉบับต่อปี มีวงเงินรวมกันกว่า 1.35 ล้านล้านบาท นอกจากบริการ e-LG on Blockchain นำเทคโนโลยี Blockchain มาใช้ในการขับเคลื่อนกลุ่มธุรกิจอื่น ๆ ได้ เช่น การขอหนังสือรับรองสินค้าอิเล็กทรอนิกส์ เพื่อขอจัดลำดับชั้นผู้ประกอบการงานก่อสร้างกับกรมบัญชีกลาง โดยผู้ประกอบการสามารถส่งเอกสารได้ที่ธนาคารที่ให้บริการ และสามารถรอรับผลการอนุมัติผ่านทางระบบ e-GP ของกรมบัญชีกลางได้โดยตรง การขอหนังสือรับรองสินค้าอิเล็กทรอนิกส์จะช่วยลดความผิดพลาดในการตรวจสอบข้อมูลและออกหนังสือรับรองได้เร็วขึ้น



นอกจากนี้ได้มีการเปิดตัวโครงการหนังสือรับรองทางการเงินอิเล็กทรอนิกส์ผ่านระบบบล็อกเชน หรือ Bank Confirmation on Blockchain ที่เกิดจากความร่วมมือของหลายหน่วยงาน อาทิ ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ บริษัทผู้สอบบัญชี และบริษัทชั้นนำ เพื่อช่วยแก้ปัญหาและลดระยะเวลาในการขอหนังสือรับรองทางการเงิน ให้มีประสิทธิภาพ รวดเร็ว มีความปลอดภัยและน่าเชื่อถือ ป้องกันการปลอมแปลงข้อมูล ซึ่งเป็นการยกระดับคุณภาพของรายงานทางการเงิน และเป็นกลไกที่สำคัญในการคุ้มครองผู้ลงทุนและเสริมสร้างความน่าเชื่อถือของตลาดทุนในประเทศ

ปัจจัยความสำเร็จในการประยุกต์ใช้เทคโนโลยี Blockchain สำหรับงานบริการภาครัฐ

นอกจากการศึกษารูปแบบและความเป็นไปได้ของการนำเทคโนโลยี Blockchain มาใช้ในงานบริการต่าง ๆ ของภาครัฐแล้ว แต่การจะผลักดันให้โครงการดังกล่าวสามารถบรรลุผลได้อย่างเป็นรูปธรรมจำเป็นต้องอาศัยองค์ประกอบดังแสดงในรูปภาพที่ 18



รูปภาพที่ 23: ปัจจัยความสำเร็จในการประยุกต์ใช้เทคโนโลยี Blockchain สำหรับงานบริการภาครัฐ



การจัดตั้งคณะกรรมการแห่งชาติ The National Blockchain Council

การจัดตั้งคณะกรรมการขึ้นมาเพื่อทำหน้าที่ในการศึกษาวิจัยข้อดี ข้อเสีย รวมถึงการศึกษาความเป็นไปได้ (Feasibility Study) และข้อจำกัดภายใต้บริบทของประเทศนั้น ๆ หากมีการนำเทคโนโลยี Blockchain มาใช้ เนื่องจากการนำเทคโนโลยี Blockchain มาใช้ในงานบริการภาครัฐย่อมส่งผลกระทบต่อการเปลี่ยนแปลงกระบวนการทำงานของหน่วยงานภาครัฐไปจากเดิม ซึ่งจำเป็นต้องมีคณะกรรมการในการศึกษาวิจัยถึงผลกระทบต่าง ๆ ที่จะเกิดขึ้น รวมถึงการวางแผนรับมือหากมีการนำเทคโนโลยี Blockchain มาใช้เพื่อสนับสนุนงานบริการภาครัฐ โดยหนึ่งในกรณีศึกษาที่น่าสนใจคือรูปแบบการจัดตั้งคณะกรรมการแห่งชาติของประเทศเนเธอร์แลนด์ (Netherland) ได้มีการจัดตั้ง Dutch National Blockchain Coalition ซึ่งถูกจัดตั้งโดย The Ministry of Economy Affairs' Information Technology เป็นการจัดตั้งคณะกรรมการที่ประสานความร่วมมือในทุกภาคส่วนมากกว่า 20 หน่วยงานทั่วประเทศ ทั้งหน่วยงานภาครัฐ องค์กรด้านวิชาการ เช่นสถาบันการศึกษาและมหาวิทยาลัย รวมถึงภาคเอกชนทั้งจากสถาบันการเงิน คมนาคมขนส่งและโลจิสติกส์ และพลังงาน โดยการประสานความร่วมมือดังกล่าวมีเป้าหมายในการทำให้ประเทศเนเธอร์แลนด์ขึ้นไปอยู่แถวหน้าในการเป็นประเทศผู้นำทางด้านเทคโนโลยีนวัตกรรม (Innovative Technology) โดยเฉพาะการนำเทคโนโลยี Blockchain มาใช้ในการสร้าง Digital Identity ซึ่งคณะกรรมการดังกล่าวมีหน้าที่ในการศึกษาถึงความเป็นไปได้และข้อจำกัดผลกระทบด้านสังคม การพัฒนาทรัพยากรบุคคล (Human Capital) รวมถึงมาตรการควบคุมต่าง ๆ เพื่อสร้างความมั่นใจ ความน่าเชื่อถือ รวมถึงการรับรู้ จนนำไปสู่การยอมรับจากประชาชนในสังคมถึงการนำเทคโนโลยี Blockchain ดังกล่าวมาใช้งาน (Krawiec et al., 2016)



ประเทศไทยมีการจัดตั้งบริษัท บีซีไอ (ประเทศไทย) จำกัด หรือ BCI ภายใต้โครงการ Thailand Blockchain Community Initiative ซึ่งได้มีการจัดตั้งขึ้นในปี ค.ศ.2019 โดยเกิดจากความร่วมมือของธนาคาร รัฐวิสาหกิจ และองค์กรธุรกิจชั้นนำ ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทย โดยมีธนาคารผู้ร่วมลงทุนทั้งสิ้น 6 ธนาคาร ประกอบด้วย ธ.กรุงศรีอยุธยา, ธ.กรุงเทพ, ธ.กสิกรไทย, ธ.กรุงไทย, ธ.ไทยพาณิชย์ และ ธ.ทหารไทย เพื่อศึกษาเทคโนโลยี Blockchain และนำมาพัฒนาเป็นบริการที่จับต้องได้จริงในภาคการเงินและภาคธุรกิจ โดยมีเป้าหมาย สร้างความร่วมมือ และขยายชุมชน Blockchain ของไทย

ให้เกิดประโยชน์ในวงกว้าง สามารถรองรับบริการที่หลากหลายในอนาคต และช่วยยกระดับความสามารถในการแข่งขันทางธุรกิจ จากการใช้ประโยชน์จากโครงสร้างพื้นฐาน (shared infrastructure) และเทคโนโลยี Blockchain ร่วมกัน โดยเริ่มต้นให้บริการ หนังสือ ค้ำประกันอิเล็กทรอนิกส์ผ่านระบบบล็อกเชน (Letter of Guarantee on Blockchain : e-LG on Blockchain) ถือเป็นองค์กรแรกที่ได้รับความร่วมมือจากธนาคารพาณิชย์ รัฐวิสาหกิจ และธุรกิจขนาดใหญ่ ของประเทศไทย ในการกำหนดมาตรฐานการใช้งาน e-LG on Blockchain



นอกจากนี้ยังมีประเทศสหรัฐอาหรับเอมิเรตส์ได้จัดตั้ง The Global Blockchain Council (GBC) โดยมีนครรัฐดูไบเป็นหนึ่งในสมาชิก ซึ่งได้มีการจัดตั้งขึ้นในปี ค.ศ. 2016 ทำหน้าที่ทดสอบและผลักดันโครงการต่าง ๆ เกี่ยวกับการพัฒนาและการใช้งานเทคโนโลยี Blockchain ภายในประเทศสหรัฐอาหรับเอมิเรตส์ เพื่อให้เป็นไปตามเป้าหมายที่ต้องการผลักดันให้ประเทศสหรัฐอาหรับเอมิเรตส์กลายเป็น Smart Future ให้ทันภายในปี ค.ศ. 2020 โดยนครรัฐดูไบประเทศสหรัฐอาหรับเอมิเรตส์ (United Arab Emirates) ถือได้ว่าเป็นรัฐบาลที่มีความรอบรู้ด้านเทคโนโลยี (Tech-Savvy) ในอันดับต้น ๆ ของโลก ซึ่งประเทศสหรัฐอาหรับเอมิเรตส์ (United Arab Emirates) ถูกจัดอยู่ในอันดับที่ 2 ของโลก โดย The World Economic Forum 2016 ว่าเป็นรัฐบาลที่มีประสิทธิภาพในการนำระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมไปถึงการทำธุรกรรมผ่านออนไลน์ต่าง ๆ เพื่อให้บริการแก่ประชาชน (Breene, 2016) นครรัฐดูไบได้มีการกำหนดยุทธศาสตร์ชาติในการเป็นเมืองหลวงของเทคโนโลยี Blockchain “The Global Capital of Blockchain” ประกอบไปด้วยเป้าหมาย 3 ด้านด้วยกันคือ



การเพิ่มประสิทธิภาพการทำงานของภาครัฐ (Government Efficiency) โดยตั้งเป้าหมายในการนำเทคโนโลยี Blockchain มาใช้สำหรับการให้บริการภาครัฐแบบเต็มรูปแบบทั้งระบบ



การสร้างอุตสาหกรรมเทคโนโลยี Blockchain (Industries Creation) โดยผลักดันและสนับสนุนให้เกิดการพัฒนา Blockchain Ecosystem ขึ้นภายในประเทศ ทั้งภาคอุตสาหกรรมและภาคธุรกิจ รวมถึงบริษัท สตาร์ทอัพต่าง ๆ



การเป็นผู้นำทางด้านเทคโนโลยี Blockchain (International Leadership) โดยจัดทำโครงการนำร่องเกี่ยวกับการพัฒนา และการใช้งานเทคโนโลยี Blockchain ทั้งภายในนครรัฐดูไบ และประเทศสหรัฐอาหรับเอมิเรตส์ ภายใต้การกำกับดูแลของ The Global Blockchain Council (GBC) ซึ่งประกอบไปด้วย 7 โครงการสำคัญ ๆ ดังต่อไปนี้



โครงการที่ ①

การนำเทคโนโลยี Blockchain มาใช้ในการจัดเก็บและส่งต่อข้อมูล ประวัติการรักษาพยาบาลของผู้ป่วยเพื่อให้ผู้ที่มีส่วนเกี่ยวข้องกับกระบวนการรักษาพยาบาลสามารถเข้าถึงข้อมูลได้อย่างปลอดภัย

โครงการที่ ②

การนำเทคโนโลยี Blockchain มาใช้ในการออกใบ Certificate ให้กับเพชร โดย The Dubai Multi Commodities Centre ได้นำเทคโนโลยี Blockchain เข้ามาใช้ในการออกใบ Certificate ให้กับเพชรหรือที่รู้จักกันในชื่อ “Kimberley Certificates”

โครงการที่ ③

การนำเทคโนโลยี Blockchain มาใช้ ในการโอนกรรมสิทธิ์ โดยเฉพาะอย่างยิ่ง สินทรัพย์ที่มีสภาพคล่องต่ำ ยกตัวอย่าง เช่น ที่ดิน โดยเทคโนโลยี Blockchain สามารถเข้ามาช่วยลดขั้นตอนด้านเอกสาร และเพิ่มประสิทธิภาพกระบวนการทำ ธุรกรรมเกี่ยวกับอสังหาริมทรัพย์

โครงการที่ ④

การนำเทคโนโลยี Blockchain มาใช้ ในกระบวนการพิสูจน์ตัวตน (Identity Management) เพื่อเพิ่มประสิทธิภาพ ลดระยะเวลาในการดำเนินการทาง ธุรกรรมต่าง ๆ กับภาครัฐ

โครงการที่ ⑤

การนำเทคโนโลยี Blockchain มาใช้ในการทำพินัยกรรมดิจิทัล เพื่อโอน กรรมสิทธิ์ทรัพย์สินต่าง ๆ ให้แก่ทายาท



โครงการที่ ⑥

การนำเทคโนโลยี Blockchain มาใช้ในการสร้างโปรแกรมสะสมแต้ม เพื่อกระตุ้นการท่องเที่ยวภายในประเทศ สหรัฐอาหรับเอมิเรตส์

โครงการที่ ⑦

การนำเทคโนโลยี Blockchain มาใช้ ในการปรับปรุงกระบวนการตรวจสอบ การนำเข้าและส่งออกสินค้าระหว่าง ประเทศ โดยเฉพาะพิธีการทางเอกสาร เพื่อเพิ่มประสิทธิภาพ และความเร็ว ในการจัดส่งและชำระเงินระหว่างประเทศ

รวมถึง ประเทศสหรัฐอเมริกา โดยพบว่าในหลายรัฐ ยกตัวอย่างเช่น รัฐนิวยอร์ก รัฐเวอร์จิเนีย รัฐฮาวาย รัฐเมน และรัฐไวโอมิง ต่างก็มีการจัดตั้งคณะทำงานเกี่ยวกับเทคโนโลยี Blockchain ขึ้นมา โดยคณะทำงานดังกล่าวได้ถูก จัดตั้งขึ้นอย่างเป็นทางการ และถูกต้อง ตามกฎหมาย มีอำนาจหน้าที่ในการ ศึกษาผลกระทบต่าง ๆ ที่จะเกิดขึ้น หากมีการนำเทคโนโลยี Blockchain มาใช้สำหรับงานบริการในภาครัฐ



การสร้างระบบนิเวศของเทคโนโลยี Blockchain Blockchain Ecosystem

ในการขับเคลื่อน รวมถึงการพัฒนาต่อยอดต่าง ๆ ที่เกี่ยวข้องกับเทคโนโลยี Blockchain ให้เกิดขึ้นได้อย่างเป็นรูปธรรมและยั่งยืนนั้นมีความจำเป็นอย่างยิ่งที่จะต้องสร้างระบบนิเวศของเทคโนโลยี Blockchain ที่เอื้อต่อการพัฒนา ยกตัวอย่างเช่น นครรัฐดูไบที่ได้มีการวางนโยบายของประเทศในการนำเทคโนโลยี Blockchain มาใช้ในงานบริการภาครัฐอย่างเต็มรูปแบบ อีกทั้งยังมีการผลักดันและสนับสนุนให้เกิดการพัฒนาาระบบนิเวศที่เอื้ออำนวยต่อการพัฒนาเทคโนโลยี Blockchain ทั้งในภาคอุตสาหกรรม ภาคธุรกิจ รวมถึงบริษัทสตาร์ทอัพต่าง ๆ



การสร้างการกำกับดูแลการใช้งานเทคโนโลยี Blockchain Blockchain Governance

การประยุกต์ใช้งานเทคโนโลยี Blockchain โดยเฉพาะอย่างยิ่งในภาครัฐ มักพบปัญหาในด้านความเชื่อมั่น และการยอมรับจากสังคม ซึ่งสามารถพบเห็นได้จากหลาย ๆ โครงการนำร่องเมื่อถูกขยายผลไปสู่การใช้งานจริงในระดับประเทศ ดังนั้นในการขับเคลื่อนการใช้งานเทคโนโลยี Blockchain มีความจำเป็นอย่างยิ่งที่จะต้องสร้างกรอบ หรือมาตรการในการกำกับดูแล โดยเฉพาะอย่างยิ่งในเรื่องของกฎหมายต่าง ๆ ที่เกี่ยวข้องกับเทคโนโลยี Blockchain เพื่อให้เกิด

ความสงบเรียบร้อยในการนำเทคโนโลยี Blockchain มาใช้งาน ยกตัวอย่างเช่น ประเทศสหรัฐอเมริกา ซึ่งถือว่าเป็นอีกประเทศหนึ่งที่มีความสำคัญกับการนำเทคโนโลยี Blockchain มาใช้ในงานบริการภาครัฐ นอกจากการให้ความสำคัญในเรื่องของการนำเทคโนโลยี Blockchain มาใช้งานแล้ว ประเทศสหรัฐอเมริกายังให้ความสำคัญกับการออกกฎหมายที่เกี่ยวข้องกับเทคโนโลยี Blockchain ทั้งในระดับรัฐ (State Action) และรัฐบาลกลาง (Federal Action) โดยการออกกฎหมายที่เกี่ยวข้องกับเทคโนโลยี Blockchain ของประเทศสหรัฐอเมริกานั้น สามารถจำแนกได้เป็น 5 กลุ่มด้วยกันดังต่อไปนี้



กฎหมายว่าด้วยการจัดตั้งคณะกรรมการ / คณะทำงานเพื่อศึกษาข้อดี ข้อเสีย ข้อจำกัด รวมถึงความเป็นไปได้ของการนำเทคโนโลยี Blockchain มาใช้งาน ยกตัวอย่างเช่น รัฐนิวยอร์ก รัฐเวอร์จิเนีย รัฐฮาวาย รัฐเมน รัฐไวโอมิง และรัฐเวอร์มอนต์





กฎหมายว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์โดยใช้เทคโนโลยี Blockchain ยกตัวอย่างเช่น รัฐแคลิฟอร์เนีย รัฐเดลาแวร์ รัฐอิลลินอยส์ รัฐเทนเนสซี และรัฐเนวาดา



กฎหมายว่าด้วยการจัดเก็บข้อมูลภาครัฐในรูปแบบดิจิทัล โดยใช้เทคโนโลยี Blockchain ยกตัวอย่างเช่น รัฐแคลิฟอร์เนีย รัฐโคโรราโด รัฐแมริแลนด์ รัฐมิชิแกน รัฐนิวเจอร์ซีย์ รัฐนิวยอร์ก รัฐโอไฮโอ รัฐแอริโซนา และรัฐอิลลินอยส์



กฎหมายว่าด้วยเงินสกุลดิจิทัล (Digital Currency) ยกตัวอย่างเช่น รัฐคอนเนตทิคัต รัฐมิชิแกน รัฐเนแบรสกา และรัฐเวอร์มอนต์



กฎหมายว่าด้วยเรื่องสัญญาอัจฉริยะ (Smart Contract) ยกตัวอย่างเช่น รัฐคอนเนตทิคัต รัฐฟลอริดา รัฐเนแบรสกา รัฐนิวยอร์ก และรัฐโอไฮโอ



การกำหนดมาตรฐานเกี่ยวกับเทคโนโลยี Blockchain

ถึงแม้เทคโนโลยี Blockchain จะเป็นเทคโนโลยีที่เข้ามาเปลี่ยนแปลงรูปแบบการจัดการข้อมูลและขั้นตอนการทำธุรกรรมให้มีประสิทธิภาพมากยิ่งขึ้น ด้วยลักษณะเด่นคือการจัดเก็บข้อมูลที่มีการกระจายตัวไปยังผู้ที่อยู่ในระบบทุกคน (Nodes) แทนที่การใช้ตัวกลาง และเมื่อมีข้อมูลใหม่ก็จะอัปเดตพร้อมกันตลอดเวลา ทำให้ช่วยลดระยะเวลาการทำธุรกรรมและลดต้นทุนการดำเนินงานลงได้ อีกทั้งข้อมูลจะถูกบันทึกไว้ตั้งแต่ธุรกรรมแรกจนถึงธุรกรรมสุดท้าย

ทำให้มีความโปร่งใสและตรวจสอบได้ แต่ด้วยข้อจำกัดเกี่ยวกับกฎระเบียบ และแนวทางการพัฒนาที่มีความหลากหลาย ขาดการกำกับดูแล และรูปแบบการพัฒนาที่เป็นมาตรฐานเดียวกัน ยังคงเป็นความท้าทายสำคัญในการขยายขีดความสามารถของเทคโนโลยี Blockchain ดังนั้นในปัจจุบันพบว่ารูปแบบการพัฒนารวมไปถึงกระบวนการทางเทคนิคที่จำเป็นสำหรับการใช้เทคโนโลยี Blockchain นั้นมีความหลากหลาย และแตกต่างกันไปขึ้นอยู่กับกรอบแบบของผู้ให้บริการนั้น ๆ ซึ่งยังไม่ได้มีการกำหนดมาตรฐานออกมาในรูปแบบที่ชัดเจน ถึงแม้ว่าองค์การระหว่างประเทศว่าด้วยการกำหนดมาตรฐาน (International Organization for Standardization: ISO) ได้มีความพยายามในการกำหนดกรอบมาตรฐานสำหรับเทคโนโลยี Blockchain คือ ISO/TC 307 Blockchain and Distributed Ledger Technologies ซึ่งประกอบไปด้วย 7 หมวดด้วยกันดังต่อไปนี้



ISO/TC 307/SG 1
Reference Architecture, Taxonomy and Ontology



ISO/TC 307/SG 2
Use Cases



ISO/TC 307/SG 3
Security and Privacy



ISO/TC 307/SG 4
Identity



ISO/TC 307/SG 5
Smart Contracts



ISO/TC 307/SG 6
Governance of Blockchain and Distributed Ledger
Technology Systems



ISO/TC 307/SG 7
Interoperability of Blockchain and Distributed Ledger
Technology Systems



แต่ความพยายามในการกำหนดมาตรฐานดังกล่าวนั้นยังอยู่ในขั้นตอนของการเตรียมการ และการจัดประชุมระหว่างคณะกรรมการยกร่างมาตรฐาน โดยคาดการณ์ว่าจะมีการประกาศใช้อย่างเป็นทางการภายในปี ค.ศ. 2021 (Morris, 2018) ทั้งนี้พบว่าในหลายประเทศผู้นำด้านเทคโนโลยี Blockchain ต่างก็เริ่มศึกษาเกี่ยวกับการกำหนดมาตรฐานด้านเทคโนโลยี Blockchain ของตนเองเพื่อให้สอดคล้องกับมาตรฐาน ISO/TC 307 Blockchain and Distributed Ledger Technologies ยกตัวอย่างเช่น ประเทศจีน ได้มีการ

จัดทำมาตรฐานเทคโนโลยี Blockchain เพื่อประกาศใช้ภายในประเทศ เพื่อรองรับการขยายตัวของเทคโนโลยี Blockchain โดยเฉพาะอย่างยิ่งการยกระดับมาตรฐานเทคโนโลยี Blockchain ซึ่งถูกพัฒนาเพื่อใช้งานในระดับประเทศ ไปสู่การพัฒนาอุตสาหกรรมเทคโนโลยี Blockchain ให้เป็นไปตามมาตรฐานสากล ดังนั้นการกำกับดูแล และรูปแบบการพัฒนาที่เป็นมาตรฐานเดียวกัน จึงยังคงเป็นความท้าทายสำคัญในการขยายขีดความสามารถของเทคโนโลยี Blockchain ต่อไปในอนาคต



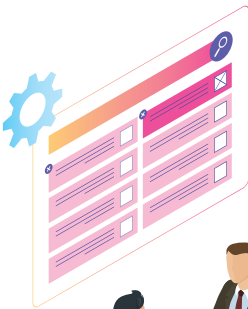


การพัฒนาบุคลากรที่มีความรู้ความสามารถด้านเทคโนโลยี Blockchain (Capacity Building)

ปัจจัยที่สำคัญอีกประการหนึ่งของการขับเคลื่อนเทคโนโลยีเกิดใหม่ให้ประสบความสำเร็จได้เป็นอย่างดีเป็นรูปธรรม คือการพัฒนาบุคลากรที่มีความรู้ความสามารถในเทคโนโลยีนั้น ๆ สำหรับเทคโนโลยี Blockchain ก็เช่นเดียวกัน โดยสถานการณ์ด้านบุคลากรของเทคโนโลยี Blockchain ในปัจจุบันถือว่ายังขาดแคลนอยู่เป็นจำนวนมาก ซึ่งเป็นเรื่องท้าทายที่จะต้องได้รับการพัฒนาต่อไปในอนาคต

ทั้งนี้พบว่าหลายประเทศที่มีแนวนโยบายในการเป็นผู้นำด้านเทคโนโลยี Blockchain ได้ตระหนักถึงปัญหาดังกล่าว โดย 27 มหาวิทยาลัยชั้นนำทั่วโลกมีการจัดหลักสูตรการเรียนการสอน และหลักสูตรอบรม เพื่อพัฒนาบุคลากรให้มีความรู้ความสามารถด้านเทคโนโลยี Blockchain ให้กับประเทศต่อไป โดย 8 มหาวิทยาลัยจากจำนวนดังกล่าว คือ มหาวิทยาลัยที่อยู่ในประเทศจีน ยกตัวอย่างเช่น The Tsinghua University, Zhejiang University, and Central University of Finance and Economics ประเทศสหรัฐอเมริกา

ยกตัวอย่างเช่น Princeton University, Stanford University, and Massachusetts Institute of Technology (MIT) และอีก 5 มหาวิทยาลัยจากประเทศอังกฤษ ยกตัวอย่างเช่น University of Oxford และ University of Cambridge ส่วนที่เหลือเป็นมหาวิทยาลัยจากประเทศไซปรัส เดนมาร์ก ไอร์แลนด์ ญี่ปุ่น สิงคโปร์ และออสเตรเลีย ซึ่งหลักสูตรการเรียนการสอนส่วนใหญ่ที่เกิดขึ้นนั้นเป็นการสอนเกี่ยวกับหลักการพื้นฐานของเทคโนโลยี Blockchain เงินสกุลดิจิทัล การวิเคราะห์สถาปัตยกรรมเชิงเทคนิคของ Platform เทคโนโลยี Blockchain ที่มีอยู่ในปัจจุบัน ยกตัวอย่างเช่น Ethereum และ Hyperledger กรณีศึกษาการประยุกต์ใช้เทคโนโลยี Blockchain ในภาคส่วนต่าง ๆ รวมถึงทิศทางและแนวโน้มการพัฒนาของเทคโนโลยี Blockchain





ทั้งนี้จากการศึกษาจากแนวปฏิบัติของต่างประเทศที่เป็นผู้นำทางด้านเทคโนโลยี Blockchain ดังได้กล่าวมาแล้วข้างต้น ดังนั้นในบทถัดไปเป็นการศึกษาถึงความเป็นไปได้รวมถึงแนวทางในการนำเทคโนโลยี Blockchain มาใช้ในการให้บริการภาครัฐของประเทศไทย ซึ่งจะได้อธิบายในลำดับถัดไป



03

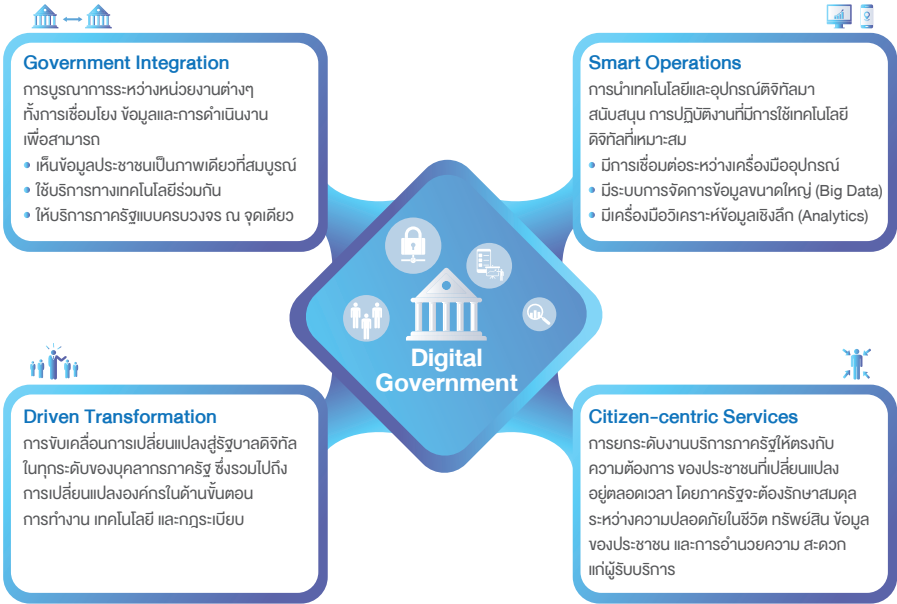
แนวคิดและหลักการประยุกต์ใช้
เทคโนโลยี Blockchain
สำหรับภาครัฐ
ภายใต้บริบทของประเทศไทย

หลักการและเหตุการณ์ประยุกต์ใช้เทคโนโลยี Blockchain สำหรับภาครัฐไทย



แนวคิดในการนำเทคโนโลยี Blockchain มาประยุกต์ใช้สำหรับภาครัฐไทยนั้น เกิดจากแนวคิดที่ต้องการ “ยกระดับภาครัฐไทยสู่การเป็นรัฐบาลดิจิทัลที่มีการบูรณาการระหว่างหน่วยงาน มีการทำงานแบบอัจฉริยะ ให้บริการโดยมีประชาชนเป็นศูนย์กลาง และขับเคลื่อนให้เกิดการเปลี่ยนแปลงได้อย่างแท้จริง” ซึ่งแนวคิดดังกล่าวเป็นวิสัยทัศน์การพัฒนารัฐบาลดิจิทัลของประเทศไทย ตาม (ร่าง) แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2560-2564 ในการยกระดับขีดความสามารถเชิงดิจิทัลของภาครัฐไทยสู่การเป็นรัฐบาลดิจิทัลดังวิสัยทัศน์ที่กำหนดไว้ นั้น ต้องอยู่บนพื้นฐานการดำเนินการ 4 ประการ ได้แก่ การบูรณาการภาครัฐ (Government Integration) การดำเนินงานแบบอัจฉริยะ (Smart Operation) การให้บริการโดยมีประชาชนเป็นศูนย์กลาง (Citizen-Centric Services) และการสนับสนุนให้เกิดการขับเคลื่อนไปสู่การเปลี่ยนแปลง (Driven Transformation) ดังแสดงในรูปภาพที่ 19

ยกระดับภาครัฐไทยสู่การเป็นรัฐบาลดิจิทัลที่มีการบูรณาการระหว่างหน่วยงาน
 มีการทำงานแบบอัจฉริยะ ให้บริการโดยมีประชาชนเป็นศูนย์กลาง
 และขับเคลื่อนให้เกิดการเปลี่ยนแปลงได้อย่างแท้จริง



รูปภาพที่ 24: วิสัยทัศน์รัฐบาลดิจิทัล

ที่มา: สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน), (2560)





1

การบูรณาการภาครัฐ Government Integration

การบูรณาการภาครัฐ (Government Integration) คือ การบูรณาการระหว่างหน่วยงานรัฐต่าง ๆ ตั้งแต่การเชื่อมโยงข้อมูล บริการ ไปจนถึงการดำเนินงาน เพื่อยกระดับประสิทธิภาพในการปฏิบัติงานและการให้บริการของรัฐ ทั้งในระดับหน่วยงานย่อยไปจนถึงระดับ

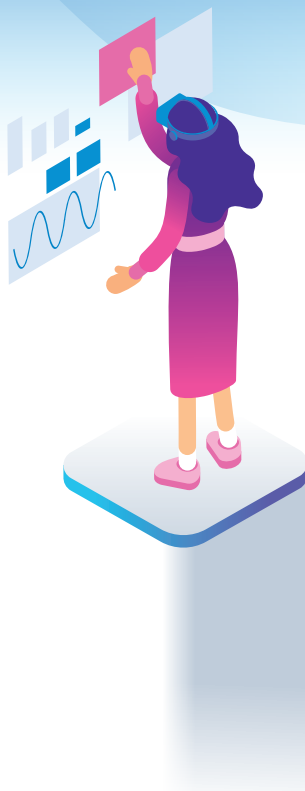
กระทรวง ซึ่งการเกิดการบูรณาการภาครัฐดังกล่าวจะทำให้รัฐบาลตระหนักถึงความต้องการและความจำเป็นในการนำเทคโนโลยีมาปรับใช้กับการดำเนินงานต่าง ๆ ในแต่ละหน่วยงาน เพื่อลดความซ้ำซ้อนในด้านการเบิกจ่ายงบประมาณ ระยะเวลาการดำเนินการ หรือแม้แต่การดูแลรักษาระบบต่าง ๆ อีกทั้งยังเพิ่มประสิทธิภาพจากการใช้บริการทางเทคโนโลยีร่วมกัน (Share Services) และการประหยัดต่อขนาด (Economies of Scale) ในการลงทุนโครงสร้างพื้นฐานกลาง นอกจากนี้การบูรณาการภาครัฐยังนำไปสู่การให้บริการภาครัฐแบบครบวงจร ณ จุดเดียว (One stop Service) ที่สามารถตอบโจทย์ด้านการอำนวยความสะดวกแก่ประชาชนได้มากยิ่งขึ้น

2

การดำเนินงานแบบอัจฉริยะ: Smart Operation

การดำเนินงานแบบอัจฉริยะ (Smart Operation) คือ การนำเทคโนโลยีและอุปกรณ์ดิจิทัลที่เหมาะสมมาสนับสนุนการปฏิบัติงานของเจ้าหน้าที่ภาครัฐไทย เพื่อให้สามารถดำเนินงานอย่างถูกต้อง แม่นยำ รวดเร็ว และตรงจุดมากขึ้น โดยมีการเชื่อมต่อระหว่างเครื่องมืออุปกรณ์ (Internet of Things) ต่างๆ อย่างทั่วถึง ทำให้เจ้าหน้าที่สามารถสื่อสารแลกเปลี่ยนข้อมูลกันได้เป็นปัจจุบัน และมีประสิทธิภาพมากขึ้น ยิ่งไปกว่านั้นอาจมีการเชื่อมต่อเครื่องมืออุปกรณ์ให้สื่อสารถึงกันแบบอัตโนมัติ โดยไม่ต้องอาศัยการควบคุมของเจ้าหน้าที่ตลอดเวลา ซึ่งเมื่อนำระบบการจัดการข้อมูลขนาดใหญ่ (Big Data) มาช่วยจัดระเบียบฐานข้อมูล ประกอบกับนำเครื่องมือวิเคราะห์ข้อมูลเชิงลึก

(Analytics) มาช่วยทำความเข้าใจข้อมูลอย่างลึกซึ้ง จะช่วยทำให้เจ้าหน้าที่ภาครัฐไทยสามารถคาดการณ์ล่วงหน้า เพื่อสนับสนุนการตัดสินใจ และหน่วยงานภาครัฐไทยสามารถจัดทำบริการแบบเชิงรุกได้อย่างมีประสิทธิภาพ



3

การให้บริการโดยมีประชาชนเป็นศูนย์กลาง Citizen-centric Services

การให้บริการโดยมีประชาชนเป็นศูนย์กลาง (Citizen-centric Services) คือ การยกระดับงานบริการภาครัฐให้ตรงกับความต้องการของประชาชนที่เปลี่ยนแปลงอยู่ตลอดเวลา โดยภาครัฐไทยจะต้องรักษาสมดุลระหว่างความปลอดภัยในชีวิตทรัพย์สิน ข้อมูลของประชาชน และการอำนวยความสะดวก (Rebalancing between Security & Facilitation) ตลอดจนกำหนดระดับ

การรักษาความปลอดภัยและระดับความเข้มงวดของการยืนยันพิสูจน์ตัวตนให้เหมาะสมกับความซับซ้อนของงานบริการ ประเภทของงานบริการ และกลุ่มผู้รับบริการต่าง ๆ



4

การสนับสนุนให้เกิดการขับเคลื่อน ไปสู่การเปลี่ยนแปลง Driven Transformation



การสนับสนุนให้เกิดการขับเคลื่อนไปสู่การเปลี่ยนแปลง (Driven Transformation) คือการวางแนวทางการขับเคลื่อนภาครัฐไทยสู่การเป็นรัฐบาลดิจิทัลในทุกกระดับของบุคลากรภาครัฐ โดยอาศัยกระบวนการทัศน์การเปลี่ยนแปลงโดยมุ่งเน้นผลสัมฤทธิ์ (Outcome-driven Transformation) ที่มีการปรับเปลี่ยนแปลงองค์กรแบบครบวงจร (End-to-End Transformation) ทั้งในด้านทรัพยากรมนุษย์ (People) ขั้นตอนการทำงาน (Process) เทคโนโลยี (Technology)

และกฎระเบียบ (Regulation) รวมทั้งมีการขับเคลื่อนโดยมีการบริหารจัดการโครงการและการกำกับดูแล (Project Management and Governance) ที่ชัดเจน ภายใต้การสนับสนุนของผู้นำระดับประเทศที่มีความมุ่งมั่น มีวิสัยทัศน์และเล็งเห็นความสำคัญของการนำเทคโนโลยีมาใช้ในการพัฒนาประเทศอย่างแท้จริง (Change Leadership) อันจะส่งผลให้ภาครัฐสามารถดำเนินงานตั้งแต่ต้นจนจบกระบวนการได้อย่างไร้รอยต่อ

ทั้งนี้เพื่อให้การขับเคลื่อนสู่การเป็นรัฐบาลดิจิทัลได้อย่างเป็นรูปธรรมนั้นจำเป็นต้องอาศัยเทคโนโลยี และนวัตกรรมในการขับเคลื่อน โดยใน (ร่าง) แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2560-2564 ได้มีการกล่าวถึงแนวโน้มของเทคโนโลยีสำคัญที่มีผลต่อการขับเคลื่อนไปสู่การเป็นรัฐบาลดิจิทัลที่สำคัญไว้ 9 เทคโนโลยีด้วยกัน ดังแสดงในรูปภาพที่ 20



รูปภาพที่ 25: แนวโน้มเทคโนโลยีที่สำคัญสำหรับการพัฒนารัฐบาลดิจิทัล

ที่มา: สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน), (2560)



โดยส่วนราชการต่าง ๆ ทั้งในระดับสำนัก กรม หรือกระทรวง สามารถที่จะนำเทคโนโลยีและนวัตกรรมเหล่านี้เข้ามาปรับใช้กับการทำงานของภาครัฐ ตลอดจนใช้พัฒนาบริการ หรือกระบวนการดำเนินงานต่าง ๆ ได้ โดยจะเห็นได้ว่าเทคโนโลยี Blockchain หรือ Distributed Ledger Technology ถือเป็น 1 ใน 9 เทคโนโลยีสำคัญในการขับเคลื่อนไปสู่การพัฒนารัฐบาลดิจิทัล ด้วยคุณสมบัติของเทคโนโลยี Blockchain ในการจัดเก็บข้อมูลและใช้ประโยชน์จากเครือข่ายเพื่อตรวจสอบความถูกต้อง และลดภาระการพึ่งพาคนกลางในการทำธุรกรรม ภายใต้ความปลอดภัยที่มีความน่าเชื่อถือ นอกจากการประยุกต์ใช้งานเทคโนโลยี Blockchain ในรูปแบบต่าง ๆ ดังได้กล่าวมาแล้วในบทก่อนหน้านี้ เทคโนโลยี Blockchain ยังสามารถนำมาใช้เพื่อบูรณาการบริการและการแลกเปลี่ยนข้อมูลภาครัฐได้อีกด้วย ดังแสดงในตารางที่ 3 ซึ่งเป็นการสรุปความเป็นไปได้ในการประยุกต์ใช้เทคโนโลยี Blockchain สำหรับงานบริการภาครัฐของประเทศตาม (ร่าง) แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย ทั้ง 5 ยุทธศาสตร์ ตามขีดความสามารถในด้านต่าง ๆ ดังต่อไปนี้

ตารางที่ 3: ตารางสรุปความเป็นไปได้ในการประยุกต์ใช้เทคโนโลยี Blockchain สำหรับงานบริการภาครัฐของประเทศไทย

ขีดความสามารถ	รายละเอียด	การนำเทคโนโลยี Blockchain มาประยุกต์ใช้
ยุทธศาสตร์ที่ 1: การยกระดับคุณภาพชีวิตประชาชน		
1. สวัสดิการประชาชน	บูรณาการข้อมูลประชาชนจากทุกหน่วยงาน เพื่อให้สามารถกำหนดสิทธิรายบุคคลได้อย่างถูกต้องครบถ้วน และสามารถให้บริการเชิงรุกได้	ระบบบริหารจัดการข้อมูลตัวตน ระบบการพิสูจน์และยืนยันตัวตนทางอิเล็กทรอนิกส์ (Digital Identity) ด้วยเทคโนโลยี Blockchain และระบบเบิกจ่ายสวัสดิการแบบรายบุคคลด้วย Smart Contract
2. การเพิ่มประสิทธิภาพแรงงาน	บูรณาการข้อมูลตลาดแรงงานอย่างครบวงจร เพื่อตอบสนองความต้องการทุกภาคส่วน เช่น การจัดหางาน การพัฒนาทักษะ การทราบภาพรวมตลาด	ระบบจัดเก็บข้อมูลแรงงาน รวมถึงการพิสูจน์และยืนยันตัวตนทางอิเล็กทรอนิกส์ (Digital Identity) ด้วยเทคโนโลยี Blockchain และเชื่อมโยงกับการผลิตห่วงโซ่อุปทาน (Supply Chain) การนำเข้า-ส่งออกของทั้งภาคการผลิต ภาคบริการ และภาคเศรษฐกิจดิจิทัล เพื่อสร้างประสิทธิภาพในการจัดหางานและการพัฒนาทักษะแรงงานได้อย่างเหมาะสม รวมถึงการต่อยอดระบบ Digital Identity ด้วยการบันทึกประวัติการทำงานที่ผ่านมาของแรงงาน รวมถึงความสามารถที่มีเพื่อนำไปสู่การออกใบรับรอง (Certificate) การทำงานด้วยเทคโนโลยี Blockchain
3. การศึกษา	มีระบบกลางเพื่อเชื่อมโยงงานบริการด้านการศึกษาแบบข้ามหน่วยงาน เพื่อเพิ่มความโปร่งใสและนวัตกรรมดี สำหรับงานบริการด้านการศึกษา	สร้างระบบบันทึกใบรับรอง (Certificate) ทางการศึกษาด้วยเทคโนโลยี Blockchain ที่เชื่อมโยงกับสถาบันการศึกษาทั้งในระบบและนอกระบบ รวมถึงการศึกษาแบบออนไลน์ทั้งในประเทศและต่างประเทศ ตามแนวทางของ Open Education เพื่อสร้างความน่าเชื่อถือให้กับเอกสารในการใช้เป็นหลักฐานสำหรับการเรียนต่อหรือสมัครงานได้

ขีดความสามารถ	รายละเอียด	การนำเทคโนโลยี Blockchain มาประยุกต์ใช้
4. การสาธารณสุข	มีระบบกลางเพื่อเชื่อมโยงงานบริการด้านสาธารณสุขแบบข้ามหน่วยงาน เพื่อให้การดำเนินงานด้านสาธารณสุขมีความสะดวกและรวดเร็วขึ้น	พัฒนาระบบเชื่อมโยงและแลกเปลี่ยนข้อมูลสุขภาพแห่งชาติ (National Health Information Exchange Platform) โดยใช้เทคโนโลยี Blockchain ที่เชื่อมต่อทุกหน่วยงานด้านสาธารณสุขเข้าด้วยกัน ไม่ว่าจะเป็นโรงพยาบาลรัฐ โรงพยาบาลเอกชน คลินิก หน่วยงานประกันสุขภาพภาครัฐ ประกันสุขภาพเอกชน หน่วยงานควบคุมคุณภาพ หน่วยงานวิจัย และหน่วยงานกำกับดูแล ให้สามารถเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกันได้แบบ Realtime ภายใต้มาตรฐานข้อมูลสุขภาพเดียวกัน มีส่วนติดต่อ Service ของ Application (API) ที่ครบถ้วน ยืดหยุ่น และมีความปลอดภัยสูง รวมถึงผู้ป่วยสามารถเข้าถึงข้อมูลประวัติการรักษาพยาบาลของตนได้

ยุทธศาสตร์ที่ 2: การยกระดับขีดความสามารถการแข่งขันของภาคธุรกิจ

5. การเพิ่มประสิทธิภาพภาคการเกษตร	บูรณาการข้อมูลการเกษตรระหว่างหน่วยงานเพื่อให้ได้ข้อมูลที่เหมาะสมกับเกษตรกรแบบรายบุคคล	พัฒนาระบบ Blockchain สำหรับการแลกเปลี่ยนข้อมูลจากหลายหน่วยงานที่เกี่ยวข้อง รวมทั้งข้อมูลจากอุปกรณ์ IoT ที่น่าเชื่อถือ และนำมาวิเคราะห์ร่วมกับข้อมูลเศรษฐกิจอื่น ๆ เพื่อสร้างเป็นข้อมูลและคำแนะนำที่เหมาะสมกับเกษตรกรแบบรายบุคคล รวมถึงการสร้างบริการทางการเกษตรภาครัฐด้วยเทคโนโลยี Smart Contract เพื่อให้เกษตรกร หรือหน่วยงานที่เกี่ยวข้องสามารถนำไปใช้ได้อย่างปลอดภัย เช่น สัญญาซื้อขายสินค้าเกษตรล่วงหน้าด้วย Smart Contract, Letter of Credit, Letter of Guarantee หรือกรมธรรม์ประกันภัยพิบัติด้านการเกษตร
-----------------------------------	---	--

ขีดความสามารถ	รายละเอียด	การนำเทคโนโลยี Blockchain มาประยุกต์ใช้
6. การท่องเที่ยว	ยกระดับประสบการณ์นักท่องเที่ยวในยุคดิจิทัล (Digital Tourism)	สร้างระบบ Loyalty Token ด้วยเทคโนโลยี Blockchain เพื่อใช้ในธุรกิจท่องเที่ยวและบริการของประเทศ ในการสร้างประสบการณ์ใหม่ให้กับนักท่องเที่ยวในยุคดิจิทัล อีกทั้งยังสามารถนำข้อมูลมาใช้ในการวิเคราะห์พฤติกรรมนักท่องเที่ยวในการหาความต้องการที่แท้จริง (Unmet Need) เพื่อนำไปปรับปรุงการให้บริการ และวิเคราะห์หาข้อมูลเชิงลึก (Insight) เพื่อนำไปสร้างบริการรูปแบบใหม่ที่สามารถตอบสนองความต้องการนักท่องเที่ยวได้อย่างแท้จริง รวมถึงการเชื่อมโยงข้อมูลจากหน่วยงานต่าง ๆ ยกตัวอย่างเช่น ข้อมูลการยืนยันตัวตนทางอิเล็กทรอนิกส์ (Digital Identity) ข้อมูลสุขภาพของนักท่องเที่ยว ผ่านสายการบินและระบบตรวจคนเข้าเมือง โดยใช้เทคโนโลยี Blockchain เพื่อยกระดับการให้บริการนักท่องเที่ยวได้อย่างมีประสิทธิภาพ
7. การลงทุน	มีระบบกลางเพื่อเชื่อมโยงงานบริการด้านการลงทุนระหว่างหน่วยงานผู้มีอำนาจในการอนุมัติเพื่อขอใบอนุญาตเริ่มต้นธุรกิจ	พัฒนาระบบ Blockchain เพื่อเชื่อมโยงหน่วยงานด้านการลงทุน ภายในประเทศจากผู้ประกอบการทั้งในและต่างประเทศ รวมถึงการสนับสนุนให้ผู้ประกอบการไทยไปลงทุนยังต่างประเทศ โดยใช้ Smart Contract ในกระบวนการขออนุญาตและอนุมัติ เพื่อสร้างความโปร่งใสและตรวจสอบได้
8. การค้า (นำเข้า/ส่งออก)	มีระบบบูรณาการนำเข้า/ส่งออก แบบครบวงจร เพื่อให้ผู้ประกอบการสามารถทำธุรกรรมที่เกี่ยวข้องกับการนำเข้า/ส่งออกได้	พัฒนาระบบ Blockchain โดยใช้ Smart Contract ในการสร้างบริการภาครัฐเกี่ยวกับการนำเข้า/ส่งออก เช่น บริการชำระเงิน, บริการ Escrow, การออกใบรับรองแหล่งกำเนิดของสินค้า (Certificate of Origin), ตราสารเครดิต (Letter of Credit: LC), หนังสือค้ำประกัน (Letter of Guarantee: LG), สินเชื่อ Factoring, Trade Finance โดยร่วมมือกับธนาคารรัฐและเอกชน

ขีดความสามารถ	รายละเอียด	การนำเทคโนโลยี Blockchain มาประยุกต์ใช้
9. วิสาหกิจขนาดกลางและขนาดย่อม	มีระบบบูรณาการเชิงรุกเพื่อให้ข้อมูลความรู้และคำปรึกษาสำหรับการประกอบธุรกิจ แก่ SME แบบครบวงจร ณ จุดเดียว โดยมีภาครัฐเป็นผู้สนับสนุนระบบ ICT	พัฒนาระบบ Blockchain เพื่อเชื่อมโยงหน่วยงานด้านวิสาหกิจขนาดกลางและขนาดย่อม โดยใช้ Smart Contract ในการสร้างบริการภาครัฐเกี่ยวกับวิสาหกิจขนาดกลางและขนาดย่อม เช่น การติดตามผลการให้ทุนสนับสนุน ระบบสิทธิบัตร และการต่อยอดนวัตกรรม
10. ภาษีและรายได้	มีการบูรณาการข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องเพื่อเพิ่มขีดความสามารถในงานบริการด้านภาษี	พัฒนาระบบ Blockchain เพื่อเชื่อมโยงหน่วยงานที่กำกับดูแลด้านภาษี และการฟอกเงิน โดยปรับเปลี่ยนขั้นตอนการชำระภาษีจากแบบยื่นรายเดือนหรือรายปี เป็นการเก็บแบบอัตโนมัติด้วย Smart Contract เพื่อลดขั้นตอนการจัดเก็บภาษี และการตรวจสอบบัญชี
11. การคมนาคม	มีการบูรณาการข้อมูลด้านคมนาคมในการอำนวยความสะดวกและเพิ่มความปลอดภัยต่อภาคธุรกิจและภาคประชาชน	พัฒนาระบบเชื่อมโยงข้อมูลผู้ขับขี่ ประวัติผู้ขับขี่ และข้อมูลพาหนะ และตำแหน่ง โดยผสานการทำงานระหว่างเทคโนโลยี Blockchain และ IoT
12. สาธารณูปโภค	มีระบบกลางเพื่อเชื่อมโยงงานบริการด้านสาธารณูปโภคระหว่างหน่วยงานเพื่อเพิ่มประสิทธิภาพการให้บริการด้านสาธารณูปโภคที่มีประสิทธิภาพมากยิ่งขึ้น	พัฒนาระบบ Blockchain เพื่อเชื่อมโยงงานบริการด้านสาธารณูปโภคระหว่างหน่วยงาน โดยนำ Smart Contract มาใช้ในขั้นตอนการขอรับบริการและการชำระเงิน เพื่อสร้างความโปร่งใสและตรวจสอบได้

ยุทธศาสตร์ที่ 3: การยกระดับความมั่นคงและความปลอดภัย

<p>13. ความปลอดภัยสาธารณะ</p>	<p>บูรณาการข้อมูลจากกล้องวงจรปิดเพื่อเฝ้าระวังและตรวจจับความเสี่ยงก่อนเกิดเหตุ โดยบริหารจัดการผ่านระบบศูนย์บัญชาการ</p>	<p>พัฒนาระบบ Identity และ Authentication ของกล้องวงจรปิดภาครัฐ รวมถึงการอนุญาตให้กล้องวงจรปิดของภาคเอกชนสามารถเข้าร่วมได้ โดยใช้เทคโนโลยี Blockchain อีกทั้งยังสามารถนำเทคโนโลยี Blockchain มาใช้กับร่วมกับระบบ Preventive Maintenance ในการกำหนดการซ่อมบำรุง โดยใช้ Smart Contract</p>
<p>14. การบริหารจัดการชายแดน</p>	<p>ขยายผลจากระบบพิสูจน์ตัวตนด้วยลายนิ้วมือให้ครอบคลุมทุกด้านสามารถรองรับพลเมืองและชาวต่างชาติที่มีการลงทะเบียน</p>	<p>การเชื่อมโยงข้อมูล Identity ข้อมูล Biometric และข้อมูลสุขภาพของผู้ผ่านแดน จากระบบตรวจคนเข้าเมือง ศูนย์ควบคุมโรค หน่วยงานป้องกันการก่อการร้ายข้ามชาติ ผ่านเทคโนโลยี Blockchain เพื่อเพิ่มความสะดวกรวดเร็วในการทำงานของเจ้าหน้าที่</p>
<p>15. การป้องกันภัยธรรมชาติ</p>	<p>ระบบวิเคราะห์และคาดการณ์ภัยธรรมชาติจากข้อมูลและระบบจำลองสถานการณ์เพื่อติดตามและบริหารจัดการภัยธรรมชาติ</p>	<p>พัฒนาระบบ Blockchain เพื่อใช้ในการแลกเปลี่ยนข้อมูลจากหลายหน่วยงานที่เกี่ยวข้องรวมทั้งข้อมูลจากอุปกรณ์ IoT ที่น่าเชื่อถือและนำมาวิเคราะห์ร่วมกับโมเดลการพยากรณ์ โดยสร้างข้อมูลที่น่าเชื่อถือ (Oracle) สำหรับการจัดทำระบบจำลองสถานการณ์เพื่อติดตามและบริหารจัดการภัยธรรมชาติ</p>
<p>16. การจัดการในภาวะวิกฤต</p>	<p>บูรณาการข้อมูลจากหน่วยงานที่เกี่ยวข้องในการติดตามและบริหารจัดการวิกฤต</p>	<p>การเชื่อมโยงข้อมูล Identity ข้อมูล Biometric ข้อมูลสุขภาพ ข้อมูลเส้นทางทางการเงิน ข้อมูลกล้องวงจรปิด เข้ากับหน่วยงานที่เกี่ยวข้องในการติดตามและบริหารจัดการภาวะวิกฤต</p>

ยุทธศาสตร์ที่ 4: การยกระดับประสิทธิภาพภาครัฐ

17. การจัดซื้อ
จัดจ้าง

มีระบบกลางในการจัดซื้อจัดจ้างภาครัฐ เพื่อให้สามารถควบคุมความโปร่งใสและเพิ่มประสิทธิภาพได้

พัฒนาระบบ Blockchain เพื่อใช้ในการเชื่อมโยงระบบ Identity ของบุคคลและนิติบุคคล เข้ากับข้อมูลคู่สัญญาที่ถูกขึ้นบัญชีดำ (Blacklist) เพื่อใช้ในกระบวนการจัดซื้อจัดจ้างภาครัฐ ยกตัวอย่างเช่น วิธีการประกวดราคา Bidding การประมูลจัดซื้อจัดจ้าง (Auction) การตรวจรับงาน และการติดตามผลการดำเนินงาน และออกรายงานประจำปีของแต่ละหน่วยงานด้วย Smart Contract



ดังนั้นหากมีการนำเทคโนโลยี Blockchain มาใช้เพื่อสนับสนุนการบูรณาการบริการและแลกเปลี่ยนข้อมูลภาครัฐจริง จะสามารถช่วยสนับสนุนโครงการต่าง ๆ ที่สำนักงานพัฒนารัฐบาลดิจิทัล (สพร.) กำลังดำเนินการอยู่ได้ ยกตัวอย่างเช่น

1

ระบบยืนยันตัวบุคคลกลาง e-Authentication Service

ระบบยืนยันตัวบุคคลกลาง (e-Authentication Service) เพื่อให้ประชาชน และเจ้าหน้าที่ของหน่วยงานภาครัฐสามารถเข้าถึงระบบสารสนเทศต่าง ๆ ของรัฐ ทั้งที่เป็นระบบบริการอิเล็กทรอนิกส์ภาครัฐ (e-Service) และระบบงานภายในของภาครัฐ (Back Office) ได้ โดยมีการควบคุมและรักษาความปลอดภัยด้วยมาตรการอันเหมาะสม นอกจากนี้ระบบยืนยันตัวบุคคลดังกล่าว ยังรองรับการเข้าถึงระบบงานแบบรวมศูนย์ (Single Sign-On: SSO) เพื่อให้ผู้ใช้งานสามารถลงชื่อเข้าใช้งานระบบบริการอิเล็กทรอนิกส์ภาครัฐ (e-Service) ต่าง ๆ ได้ด้วยการ Log in ครั้งเดียวโดยไม่จำเป็นต้องลงชื่อเข้าใช้งานซ้ำอีก ทั้งนี้ระบบยืนยัน



ตัวบุคคลกลางเป็นก้าวสำคัญไปสู่การให้และรับบริการภาครัฐแบบครบวงจร จุดเดียว (One Stop Service) ในลักษณะ Single Window Entry อันจะเป็นการอำนวยความสะดวกต่อประชาชนในการเข้าถึงบริการของรัฐได้อย่างบูรณาการ

2



ศูนย์กลางแลกเปลี่ยนข้อมูลภาครัฐ Government Data Exchange Center : GDx

ศูนย์กลางแลกเปลี่ยนข้อมูลภาครัฐ (Government Data Exchange Center : GDx) เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลและเอกสารทะเบียนดิจิทัลระหว่างหน่วยงานภาครัฐ เพื่ออำนวยความสะดวกแก่ประชาชนและภาคเอกชน เมื่อใช้บริการจากภาครัฐ ช่วยให้หน่วยงานภาครัฐสามารถแลกเปลี่ยนเชื่อมโยงข้อมูลในรูปแบบดิจิทัล และเมื่อภาครัฐสามารถแลกเปลี่ยนข้อมูลในรูปแบบดิจิทัลได้ จึงไม่จำเป็นต้องใช้สำเนาเอกสารในรูปแบบกระดาษต่อไป โดยในระยะแรกจะเริ่มนำร่องกับบริการภาครัฐที่มีการเรียกขอสำเนาบัตรประจำตัวประชาชน สำเนาทะเบียนบ้าน ภายใต

“โครงการยกเลิกสำเนาเอกสาร” และขยายผลไปสู่บริการยกเลิกเรียกขอเอกสารทะเบียนดิจิทัล/ใบอนุญาตอื่น ๆ ต่อไป



การประยุกต์ใช้เทคโนโลยี Blockchain เพื่อการบูรณาการบริการและแลกเปลี่ยนข้อมูลภาครัฐ



ระบบบริการอิเล็กทรอนิกส์ (e-Service) ของภาครัฐไทยในปัจจุบันส่วนใหญ่ยังขาดการบูรณาการเพื่อเชื่อมโยงเข้ากับระบบบริการอิเล็กทรอนิกส์ (e-Service) ของหน่วยงานอื่น ๆ ทำให้ประชาชนที่มาติดต่อหน่วยงานราชการต่าง ๆ ไม่ได้รับความสะดวกเท่าที่ควร อีกทั้งยังจำเป็นต้องใช้สำเนาหลักฐานในการเข้ารับบริการ ดังนั้นกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมหรือกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้จัดทำ กรอบแนวทางเชื่อมโยงรัฐบาลอิเล็กทรอนิกส์แห่งชาติ เวอร์ชัน 2.0 เพื่อให้เกิดการพัฒนาบริการร่วม e-Service ให้สามารถให้บริการภาครัฐแบบครบวงจร ณ จุดเดียว (One Stop Service)

โดยใช้สถาปัตยกรรมการออกแบบเชิงบริการ Services Oriented Architecture (SOA) เป็นแนวทางการเชื่อมโยงและแลกเปลี่ยนข้อมูลของระบบต่าง ๆ ภายในหน่วยงานและระหว่างหน่วยงาน พัฒนา Web Service สำหรับระบบงานภายในของหน่วยงาน และใช้ช่องทางการสื่อสารทำหน้าที่เป็นตัวกลางเชื่อมระหว่าง Web Service ต่าง ๆ ที่หน่วยงานรัฐที่จัดทำขึ้น ทั้งฝ่ายให้บริการ (Service Provisioning) และฝ่ายรับบริการ(Service Consumption) โดยใช้ API ในการส่งข้อมูลผ่าน Enterprise Service Bus (ESB) เป็นเครื่องมือช่วยลดอุปสรรคของความหลากหลายของเทคโนโลยีการเชื่อมโยงข้อมูลในการเปิดช่องทางบริการให้เป็นมาตรฐานเดียวกันในการสื่อสารกับระหว่าง Web Service ของหน่วยงานภาครัฐดังแสดงในรูปภาพที่ 21

รูปภาพที่ 26: ระบบบูรณาการการให้บริการภาครัฐโดยใช้ Enterprise Service Bus (ESB)

ที่มา: ปรับปรุงจาก (Marchionni, 2018)





ข้อควรพิจารณาการออกแบบสถาปัตยกรรมการส่งข้อมูลผ่าน
Enterprise Service Bus (ESB) มีดังนี้

- 1 การเปลี่ยนแปลงหรือปรับปรุงจากกระบวนการทำงานของ e-Service ที่ให้บริการ (และบริการที่เกี่ยวข้อง) อาจมีผลต่อหน่วยงานที่ใช้ e-Service นั้น ยกตัวอย่างเช่น เมื่อผู้ให้บริการดำเนินการปรับปรุง เปลี่ยนแปลงเทคโนโลยี ที่ใช้ภายในตัวบริการหรืออุปกรณ์เชื่อมต่อ Firewall
- 2 ทุกครั้งที่มีการเรียกใช้ e-Service กับบริการอื่น ๆ ต้องทำการตรวจสอบ ความสมบูรณ์ของการป้อนข้อมูลหรือทุกพารามิเตอร์ที่เกิดขึ้น ทำให้ต้องใช้เวลาเพิ่มขึ้น และเครื่องแม่ข่ายทำงานหนักขึ้นทำให้ลดประสิทธิภาพโดยรวม
- 3 การบูรณาการระหว่างหน่วยงานอาจกลายเป็นกระบวนการที่ซับซ้อน เนื่องจากความแตกต่างของระบบรักษาความปลอดภัยและข้อกำหนด (แม้ว่า Enterprise Service Bus จะทำงานได้อย่างถูกต้อง)

- 4 ต้องมีการแลกเปลี่ยนใบรับรอง เช่น Certificate Authority (CA) เพื่อรับรองว่าได้ให้ไว้ซึ่งเอกสารที่น่าเชื่อถือ
- 5 การลงทุนด้านโครงสร้างพื้นฐานที่มีราคาแพงสำหรับการจัดเตรียมการให้บริการและความปลอดภัยภายในหน่วยงาน
- 6 แต่ละหน่วยงานต้องมีการตั้งทีมสนับสนุน (ตาม SLA ที่ตกลง) เพื่อรองรับความล้มเหลวในการให้บริการ
- 7 กระบวนการพัฒนา Service ที่ต้องมีการเชื่อมโยงข้อมูลระหว่างหน่วยงาน มีขั้นตอนและใช้ระยะเวลาในการดำเนินงานมาก เช่น การทำบันทึกข้อตกลงร่วมกัน (MOU) การศึกษากระบวนการหรืออาจต้องทำการปรับเปลี่ยนกระบวนการทำงานของหน่วยงานเพื่อการเชื่อมโยงข้อมูล การรับส่งข้อมูล การพัฒนาระบบ และการทดสอบระบบ



ดังนั้นการนำเทคโนโลยี Blockchain มาใช้ในการเชื่อมโยงงานบริการภาครัฐ แทนการใช้ Enterprise Service Bus (ESB) ดังแสดงในรูปภาพที่ 22



รูปภาพที่ 27: การเชื่อมโยงบูรณาการการให้บริการภาครัฐโดยใช้เทคโนโลยี Blockchain

ที่มา: ปรับปรุงจาก (Marchionni, 2018)



โดยเป็นการเชื่อมต่อกันเป็นเครือข่ายแบบ Peer-to-Peer และใช้ APIs ของ Node แต่ละตัวเชื่อมกับ Web Service ที่หน่วยงานจัดเตรียมไว้ในการเชื่อมโยงกับฐานข้อมูลทะเบียนของหน่วยงานในเครือข่าย Blockchain โดยแต่ละ Node จะทำการจัดเก็บข้อมูลชุดเดียวกัน และใช้กระบวนการ Consensus ในการตรวจสอบความถูกต้อง ก่อนทำการจัดเก็บข้อมูลลง Block ทั้งนี้รูปแบบการจัดเก็บข้อมูลลงใน Blockchain อาจอยู่ในรูปแบบ On Chain⁷ หรือ Off Chain ตามความเหมาะสมในการออกแบบ และมี CA (Certification

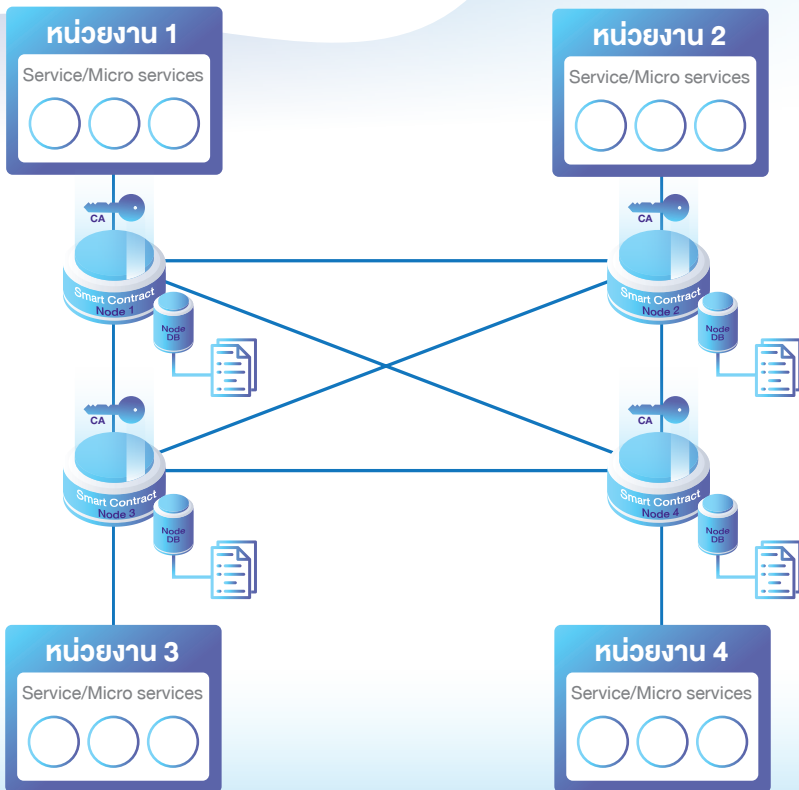
Authority) ในการรับรองรายการธุรกรรมว่าเป็นธุรกรรมของหน่วยงานนั้นจริง ทั้งนี้หน่วยงานแต่ละหน่วยงานจะต้องมี Node ซึ่งอาจจะอยู่ในรูปแบบ Light Node หรือ Full Node ติดตั้งอยู่ในเครือข่าย Blockchain เมื่อมีการเรียกใช้บริการระบบจะทำการแจกจ่าย Smart Contract ตามการ



⁷ ในระดับของ Transaction Layer สามารถแบ่งประเภทของการจัดเก็บข้อมูลบน Blockchain ได้เป็น 2 ชนิดคือ 1) “On Chain” คือการที่ข้อมูล ถูกบันทึกลง Blockchain โดยตรง 2) “Off Chain” คือการบันทึกตำแหน่งหรือตัวชี้ตำแหน่ง (Pointer) ของข้อมูลลงบน Blockchain ข้อดีของการบันทึกข้อมูลลงบน Blockchain โดยตรงนั้นคือมั่นใจได้ว่าข้อมูลจะมีความปลอดภัย อันเนื่องมาจากคุณสมบัติการทำงานของ Blockchain และข้อมูลดังกล่าวสามารถมองเห็นได้ทันทีสำหรับผู้ที่ได้รับอนุญาตให้เข้าถึงข้อมูล แต่ในเวลาเดียวกันการบันทึกข้อมูลที่ไฟล์ข้อมูลมีขนาดใหญ่ นั้นย่อมส่งผลต่อเวลาที่ใช้ในการดำเนินการสร้าง Block อย่างแน่นอน อีกทั้งอาจจะส่งผลกระทบต่อวางแผนเรื่องของขนาดระบบเพื่อรองรับข้อมูลจำนวนมากดังกล่าว ในทางตรงกันข้ามการเข้ารหัสลิงก์ หรือตัวชี้ตำแหน่งที่ข้อมูลถูกจัดเก็บอยู่แทนที่ข้อมูลจริง โดยผู้ใช้งานจะใช้ Private Key เพื่ออ่านข้อมูลใน Block ซึ่งก็คือลิงก์ หรือตำแหน่งที่จัดเก็บข้อมูลจริงเพื่อนำไปสู่การเข้าถึงข้อมูลดังกล่าวนั่นเอง ซึ่งจะเป็นการช่วยลดขนาดของข้อมูลที่ จะถูกบันทึกลงใน Block ได้ ยกตัวอย่างเช่น ฟิล์ม X-Ray และ MRI ซึ่งเป็นไฟล์รูปที่มีขนาดใหญ่จึงจำเป็นต้องเก็บเป็นลิงก์ หรือตัวชี้ตำแหน่งของข้อมูลแทน ดังนั้นองค์กรควรจะต้องพิจารณาถึงประเภทของข้อมูลด้วยในการออกแบบการจัดเก็บข้อมูลบน Blockchain

บริการที่ผู้ใช้งานเลือกใช้ในบริการนั้น ๆ ไปยัง Node ต่าง ๆ บนเครือข่าย โดย Smart Contract จะเป็นตัวกำหนดหน้าที่ของแต่ละหน่วยงานระบุไว้ ซึ่งอาจมากกว่าหนึ่งหน่วยงานก็ได้ในการดำเนินการตามเงื่อนไขที่ระบุไว้ เมื่อหน่วยงานได้ดำเนินการครบตามเงื่อนไขที่กำหนดไว้

กรณีดำเนินการเสร็จสิ้นตามสัญญา และระบบได้ตรวจสอบความถูกต้อง (Consensus) ก่อนทำการสำเนารายการการทำธุรกรรมดังกล่าวไปยัง Node ต่าง ๆ บนเครือข่าย Blockchain



รูปภาพที่ 28: องค์ประกอบทางเทคนิคการบูรณาการงานบริการภาครัฐบนเทคโนโลยี Blockchain

ที่มา: ปรับปรุงจาก (Jamsrandorj, 2017)



จากรูปภาพที่ 23 เป็นการแสดงองค์ประกอบทางเทคนิคการบูรณาการงานบริการภาครัฐบนเทคโนโลยี Blockchain ระหว่างหน่วยงานตั้งแต่สองหน่วยงานขึ้นไป เพื่อเห็นถึงองค์ประกอบและการเชื่อมต่อทางเทคนิค หลักการนี้สนับสนุนให้หน่วยงานต่าง ๆ สามารถเชื่อมต่อและสื่อสารกันได้ โดยใช้การควบคุมการเข้าถึง (Access Control System) หรือ Smart Contract ที่กระจายอยู่ตาม Node ต่าง ๆ ซึ่งแต่ละหน่วยงานจะมี Microservices, Local Storage และ Node บนเครือข่าย Blockchain ในการสื่อสารระหว่างหน่วยงานบนเครือข่าย โดยมีองค์ประกอบดังนี้

1 Access Control Application ใช้ Smart Contract เป็นตัวกำหนดสิทธิ์ในการเข้าใช้บริการ โดยแต่ละหน่วยงานสามารถกำหนดสิทธิ์ในการขอเข้าใช้บริการของหน่วยงานได้ด้วยตัวเองผ่าน Smart Contract และเรียกใช้ Services ต่าง ๆ ผ่าน APIs ได้แก่

- ❖ การกำหนด Service หรือ Microservices
- ❖ การให้สิทธิ์การเข้าถึงสำหรับ Service หรือ Microservices
- ❖ การโอนสิทธิ์การเข้าถึง
- ❖ การเพิกถอนสิทธิ์การเข้าถึง
- ❖ การให้สิทธิ์การเข้าถึงสำหรับ Service หรือ Microservices
- ❖ เรียกใช้ Service หรือ Microservices



- 2 Local Database ทุก Node จะมีฐานข้อมูลภายในใช้เป็นแหล่งจัดเก็บข้อมูลที่เกิดขึ้นบนเครือข่าย Blockchain เพื่อรับประกันว่าข้อมูลที่ถูกจัดเก็บเป็นสำเนาเดียวกัน
- 3 Services หรือ Microservices เป็นช่องทางการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างระบบงานต่าง ๆ ภายในหน่วยงานและระหว่างหน่วยงาน โดยผ่านตัว Access Control เรียกใช้
- 4 Blockchain Cluster กลุ่มเครือข่ายคอมพิวเตอร์ รูปแบบ Private และ Permission-Based Blockchain ใช้ในการแชร์ข้อมูลที่ต้องใช้ร่วมกันและเก็บประวัติรายการข้อมูลต่าง ๆ ที่เกิดจาก Access Control สามารถตรวจสอบย้อนกลับได้ แต่ไม่สามารถเปลี่ยนแปลงรายการที่ถูกบันทึกในระบบได้




จากหลักการที่ได้อธิบายไปแล้วข้างต้น ทำให้สามารถออกแบบภาพรวมการใช้เทคโนโลยี Blockchain เพื่อการบูรณาการบริการและแลกเปลี่ยนข้อมูลภาครัฐ ดังแสดงในรูปภาพที่ 24



รูปภาพที่ 29: แสดงระบบนิเวศการให้บริการหน่วยงานภาครัฐ

ที่มา: ปรับปรุงจาก (Cheng, Daub, Domeyer, & Lundqvist, 2017)



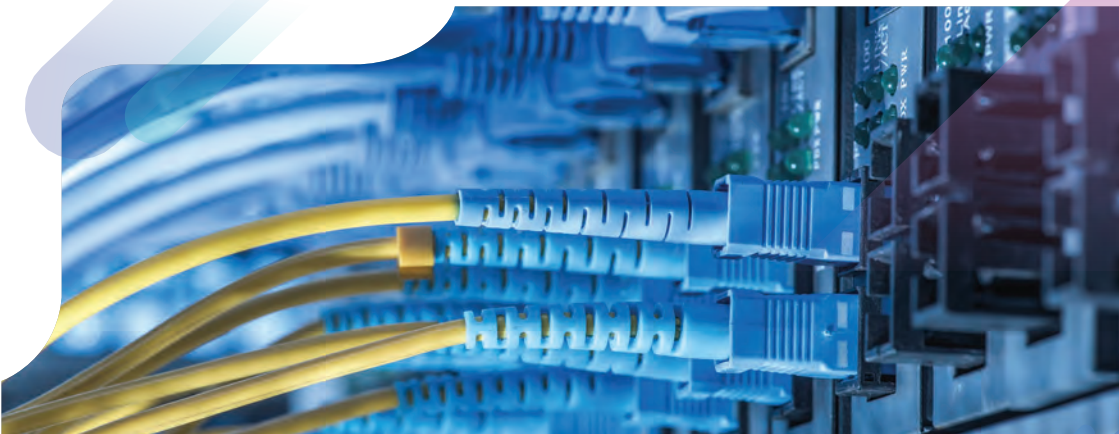
การให้บริการประชาชนสามารถเข้าถึงข้อมูลทะเบียนต่าง ๆ ของตนหรือการให้หน่วยงานรัฐสามารถแชร์ข้อมูลที่เป็นระหว่างการทำธุรกรรม รายการข้อมูลต่าง ๆ ที่เกิดขึ้นในระบบจะถูกเข้ารหัสเก็บในฐานข้อมูลเฉพาะใน Blockchain ในรูปแบบ Private หรือ Permissioned Blockchain ที่ประชาชนต้องทำการยืนยันตัวตนผ่าน เลขที่บัตรประชาชน เลขที่นิติบุคคล รหัสผ่านของผู้ใช้บริการของหน่วยงานนั้น ๆ การกำหนดสิทธิ์เข้าถึงข้อมูลเพื่อเรียกดู (อ่าน) และการเพิ่มรายการธุรกรรมใหม่ (เขียน) หรือให้หน่วยงานมีสิทธิในการอ่านหรือเปลี่ยนแปลงรายการข้อมูลธุรกรรมของประชาชนโดยใช้กุญแจสาธารณะ (Public Key) ในการแชร์ข้อมูลที่เป็นต้องตรวจสอบข้อมูลระหว่างหน่วยงานภาครัฐในการจัดทำธุรกรรมให้บริการแก่ประชาชนและกุญแจส่วนตัว (Private Key) สำหรับแก้ไขเปลี่ยนแปลงข้อมูล ผ่าน Smart Contract ซึ่งเป็นข้อตกลงสำหรับการควบคุมการดำเนินการจัดทำธุรกรรมตามที่กำหนดไว้ใน Smart Contract ของธุรกรรมนั้น ๆ เป็นกลไกในการควบคุมลำดับขั้นตอนการดำเนินการ ว่าใครจะเป็นผู้เห็น เห็นอะไรได้บ้าง เมื่อไร และดำเนินการอย่างไร

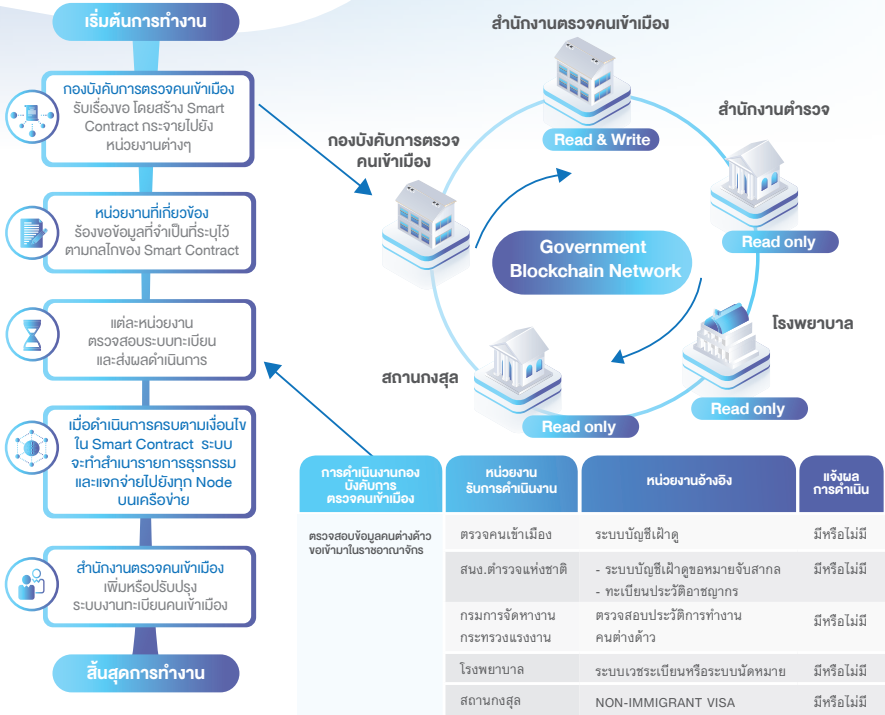


ตัวอย่างการบูรณาการงานบริการภาครัฐด้วยเทคโนโลยี Blockchain (Government Service Blockchain)

กรณีการดำเนินการขออนุญาตเข้ามาในราชอาณาจักรเป็นการชั่วคราวเพื่อเข้ารับการรักษาพยาบาลของคนต่างด้าวของเจ้าหน้าที่ประจำด่านตรวจคนเข้าเมืองที่ประจำอยู่ตามแนวชายแดน ดังแสดงในรูปภาพที่ 25

การดำเนินงานกองบังคับการตรวจคนเข้าเมือง	หน่วยงานบริการดำเนินงาน	ระบบงานอ้างอิง
ตรวจสอบข้อมูลคนต่างด้าวขอเข้ามาในราชอาณาจักร	สนง.ตรวจคนเข้าเมือง	ระบบบัญชีใฝ่ดู
	สนง.ตำรวจแห่งชาติ	- ระบบบัญชีใฝ่ดูขอหมายจับสากล - ทะเบียนประวัติอาชญากร
	กรมการจัดหางาน กระทรวงแรงงาน	ตรวจสอบประวัติการทำงานคนต่างด้าว
	โรงพยาบาล	ระบบเวชระเบียนหรือระบบนัดหมาย
	สถานกงสุล	NON-IMMIGRANT VISA





รูปภาพที่ 30: แผนภาพจำลองขั้นตอนการขออนุญาตเข้ามาในราชอาณาจักรชั่วคราว เพื่อเข้ารับการรักษาพยาบาล

ประโยชน์จากการใช้เทคโนโลยี Blockchain ในการเชื่อมโยงงานบริการภาครัฐสามารถจำแนกได้ตามผู้ใช้งาน ดังต่อไปนี้

หน่วยงานผู้ให้บริการ

- การเผยแพร่ข้อมูล (Shared Data) การเปิดข้อมูลที่จำเป็นใช้งานร่วมกัน
- การทำงานร่วมกัน (Multiple Parties) การบันทึกหรืออ่านข้อมูลจากฐานข้อมูลในการดำเนินการจัดทำรายการธุรกรรม เพื่อให้บริการเรื่องใดเรื่องหนึ่ง อาจมีหน่วยงานภาครัฐมากกว่าหนึ่งร่วมดำเนินการ โดยกำหนดพื้นที่การเข้าถึงแหล่งข้อมูลแบบ Permissionless (Public Blockchain), Permissioned (Private หรือ Consortium Blockchain)

- ❖ ไม่ต้องอาศัยตัวกลาง
- ❖ สามารถตรวจสอบ (Auditability) การบันทึกรายการธุรกรรม (จากการให้บริการ) ภายในเครือข่าย Blockchain ได้ เมื่อเขียนแล้วจะไม่สามารถเปลี่ยนแปลงหรือลบได้
- ❖ มี Access Control การกำหนดกฎเกณฑ์ต่าง ๆ ในการอนุญาตหรือปฏิเสธ เช่น รายการการร้องขอต่าง ๆ ที่เกิดขึ้นในระบบว่าจะอนุญาตหรือปฏิเสธ เช่น สิทธิการเข้าใช้ทะเบียนข้อมูล การอ่าน การเขียน การแชร์ข้อมูล ของกลไกการดำเนินทางธุรกิจที่เกี่ยวกับความสัมพันธ์ระหว่างผู้ใช้บริการกับหน่วยงานหรือระหว่างหน่วยงาน
- ❖ การดำรงอยู่ของหลักฐาน (Proof of Existence) สามารถพิสูจน์ความเป็นเจ้าของจากหลักฐานที่ได้รับการทำธุรกรรม

ผู้รับบริการ (ประชาชน หน่วยงานภาครัฐ)

- ❖ ประชาชนผู้ยื่นคำขอไม่จำเป็นต้องจัดเตรียมหลักฐานด้านเอกสารต่าง ๆ ที่มีการเก็บอยู่ระบบงานทะเบียน ๆ ของหน่วยงานภาครัฐ
- ❖ ไม่ต้องรับรองสำเนาเอกสารช่วยลดโอกาสในการทุจริต
- ❖ หน่วยงานภาครัฐแต่ละแห่งดำเนินการตามกระบวนการภายในของตนเอง
- ❖ หากมีหน่วยงานรัฐหนึ่งเปลี่ยนแปลงกระบวนการหรืออุปกรณ์ภายในหน่วยงานจะไม่มีผลกระทบต่อหน่วยงานอื่น ๆ เนื่องจาก Node แยกกันเป็นอิสระ
- ❖ ไม่มีข้อกำหนดเกี่ยวกับการเชื่อมต่อโดยตรง เนื่องจากได้รับการรับรองโดยพื้นฐานโปรโตคอลการแจกจ่ายของโปรโตคอล Blockchain และ APIs แบบมาตรฐาน
- ❖ ไม่สามารถเปลี่ยนแปลงข้อมูล

กรณีศึกษาการจัดทำระบบต้นแบบ e-Referral โดยใช้เทคโนโลยี Blockchain



การพัฒนาาระบบต้นแบบ e-Referral โดยใช้เทคโนโลยี Blockchain เกิดจากแนวคิดในการพัฒนาระบบเชื่อมโยงและแลกเปลี่ยนข้อมูลสุขภาพแห่งชาติ (National Health Information Exchange Platform) ที่เชื่อมต่อทุกหน่วยงานด้าน Healthcare เข้าด้วยกัน ไม่ว่าจะเป็นโรงพยาบาล คลินิก หน่วยงานประกัน

สุขภาพ หน่วยงานวิจัย และหน่วยงานอื่น ๆ ทั้งภาครัฐและภาคเอกชนที่เกี่ยวข้องให้สามารถเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกันได้ แบบเรียลไทม์ ภายใต้มาตรฐานข้อมูลสุขภาพเดียวกัน อีกทั้งยังจะต้องคำนึงถึงความปลอดภัย และความเป็นส่วนตัวของข้อมูลผู้ป่วย เป็นสำคัญ

โดยแนวคิดดังกล่าวอ้างอิงและสอดคล้องกับรายงานการวิเคราะห์ยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศสุขภาพ (eHealth) จัดทำโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ประจำปี 2558 ในกลยุทธ์ที่ 2: ว่าด้วยการพัฒนาคลังข้อมูลสุขภาพ โดยมีเป้าหมายส่วนหนึ่งเพื่อต้องการให้ผู้ป่วยที่ต้องส่งต่อไปรับการรักษายังสถานบริการอื่น จะต้องได้รับการรักษาอย่างต่อเนื่อง โดยสถานบริการต้นทางมีข้อมูลด้านการแพทย์และสุขภาพรายบุคคลเพื่อการกำกับติดตาม ฝ้าระวัง และดูแลปัญหาสุขภาพของประชาชนในเขตพื้นที่รับผิดชอบ ดังนั้นส่วนหนึ่งของมาตรการเพื่อให้บรรลุตามเป้าหมายที่ได้วางไว้



ก็คือการพัฒนากระบวนการแลกเปลี่ยนและส่งต่อผู้ป่วยระหว่างสถานบริการทุกระดับจะต้องมีการแลกเปลี่ยนข้อมูลทางการแพทย์เพื่อการส่งต่อผู้ป่วย (Medical Record Exchange) ทั้งแบบผู้ป่วยทั่วไปและเร่งด่วน เพื่อให้ผู้ป่วยสามารถไปรับบริการจากสถานบริการใดก็ได้

รวมถึงรายงานการวิเคราะห์ยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศสุขภาพ (eHealth) จัดทำโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ประจำปี 2560-2569 ในยุทธศาสตร์ที่ 3: ว่าด้วยการสร้างมาตรฐานของระบบข้อมูลสุขภาพ การบูรณาการข้อมูลสารสนเทศ และการเชื่อมโยงแลกเปลี่ยนข้อมูลที่มีประสิทธิภาพ โดยเฉพาะในกลยุทธ์ที่ 1: ว่าด้วยการสร้างมาตรฐานระบบข้อมูลสุขภาพที่สามารถ





แลกเปลี่ยนและเชื่อมโยง (Standards and Interoperability) กันได้อย่างมีประสิทธิภาพ รวมไปถึงยุทธศาสตร์ที่ 4: ว่าด้วยการขับเคลื่อนและพัฒนานวัตกรรมระบบบริการและโปรแกรมประยุกต์ด้าน eHealth ที่เป็นประโยชน์ต่อระบบบริการสุขภาพ (Healthcare Service Delivery) และประชาชนโดยสนับสนุนให้มีโครงการต้นแบบที่ใช้เทคโนโลยีดิจิทัลเป็นกลไกในการขับเคลื่อน eHealth ที่มีประสิทธิภาพ

ประกอบกับการขับเคลื่อนการปฏิบัติงานในระบบบริการสุขภาพให้มีประสิทธิภาพจำเป็นต้องอาศัยการแลกเปลี่ยนข้อมูลสุขภาพ (Health Information Exchange) ที่สะดวกรวดเร็วและปลอดภัย ไม่ว่าจะ เป็นเพื่อการตรวจ

รักษาผู้ป่วย การส่งต่อผู้ป่วย การเข้าถึงข้อมูลด้านสุขภาพของประชาชน การเบิกจ่ายประกันสุขภาพ การป้องกันโรคระบาด ไปจนถึงการตัดสินใจวางแผนและพัฒนานโยบายด้านสุขภาพ โดยเฉพาะในเรื่องการส่งต่อผู้ป่วย (Patient Referral) การขาดประสิทธิภาพในการแลกเปลี่ยนข้อมูลสุขภาพระหว่างโรงพยาบาลได้สร้างปัญหาตามมามากมาย ทั้งกับแพทย์ที่ไม่สามารถเข้าถึงข้อมูลทั้งหมดของผู้ป่วยได้ก่อนรับการส่งต่อ ทั้งกับผู้ป่วย และโรงพยาบาลหรือคลินิกที่มีความไม่สะดวกในการเบิกจ่าย รวมไปถึงหน่วยงานประกันสุขภาพที่ไม่สามารถติดตามและตรวจสอบการส่งต่อเพื่อนำไปปรับปรุงนโยบายและกฎระเบียบให้ดียิ่งขึ้นได้

ปัญหาหลักในปัจจุบันของระบบข้อมูลสุขภาพของประเทศซึ่งเป็นอุปสรรคต่อการแลกเปลี่ยนข้อมูลสุขภาพเกิดจากการทำงานเก็บข้อมูลซ้ำซ้อนของบุคลากรด้านสาธารณสุข การไม่มี

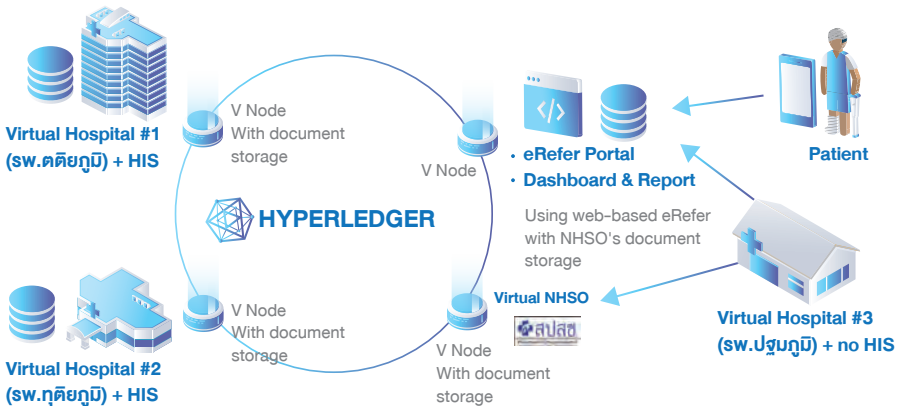
มาตรฐานของข้อมูล การไม่มีระบบกลาง แลกเปลี่ยนข้อมูลของประเทศ ปัญหาความปลอดภัยทางไซเบอร์ของการแลกเปลี่ยนข้อมูลข้ามองค์กร ปัญหาเกณฑ์การกำกับดูแลที่ไม่ชัดเจน ซึ่งปัญหานี้ไม่เพียงแต่ส่งผลกระทบต่อหน่วยงานผู้ให้บริการทางสาธารณสุขเท่านั้น ตัวประชาชนเจ้าของข้อมูลเองก็ไม่สามารถเข้าถึงและใช้ประโยชน์ ข้อมูลสุขภาพของตนเองได้อีกด้วย โดยปัญหาการแลกเปลี่ยนข้อมูลสุขภาพดังกล่าวสามารถแก้ไขได้ด้วยเทคโนโลยี Blockchain ซึ่งเป็นเทคโนโลยีที่มีศักยภาพสำหรับการเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างระบบ (Interoperability) ที่มีประสิทธิภาพ ข้อมูลมีความถูกต้อง โปร่งใส สามารถตรวจสอบได้ ซึ่งสามารถเป็นจุดเริ่มต้นของการแก้ไขปัญหาด้านข้อมูลสุขภาพของประเทศได้

ดังนั้นด้วยเหตุผลดังกล่าวไปแล้วข้างต้น สำนักงานพัฒนารัฐบาลดิจิทัล องค์การมหาชน (สปร.) จึงได้ร่วมมือกับสำนักงานหลักประกันสุขภาพแห่งชาติ เขต 13 กรุงเทพมหานคร ในการพัฒนาระบบต้นแบบ e-Referral บนเทคโนโลยี Blockchain โดยมีวัตถุประสงค์เพื่อศึกษาความเป็นไปได้ในการนำเทคโนโลยี Blockchain มาใช้เพื่อต่อยอดนวัตกรรมบริการของหน่วยงานภาครัฐ รวมถึงผลกระทบต่าง ๆ ที่เกิดขึ้นจากการใช้เทคโนโลยี Blockchain จนนำไปสู่การยกระดับภาครัฐไทยสู่การเป็นรัฐบาลดิจิทัล ที่มีการบูรณาการระหว่างหน่วยงาน ตั้งแต่การเชื่อมโยงข้อมูล การบริการ ไปจนถึงการดำเนินงานได้



ภาพรวมสถาปัตยกรรมระบบต้นแบบ e-Referral บนเทคโนโลยี Blockchain

ภาพรวมของระบบต้นแบบ e-Referral บนเทคโนโลยี Blockchain ประกอบไปด้วย Blockchain Node จำนวน 4 Node เพื่อแทน Node ของโรงพยาบาลปทุมภูมิ โรงพยาบาลทศวิทยภูมิ โรงพยาบาลตติยภูมิ และผู้บริหารระบบ ดังแสดงในรูปภาพที่ 26



รูปภาพที่ 31: ภาพรวมสถาปัตยกรรมระบบต้นแบบ e-Referral บนเทคโนโลยี Blockchain

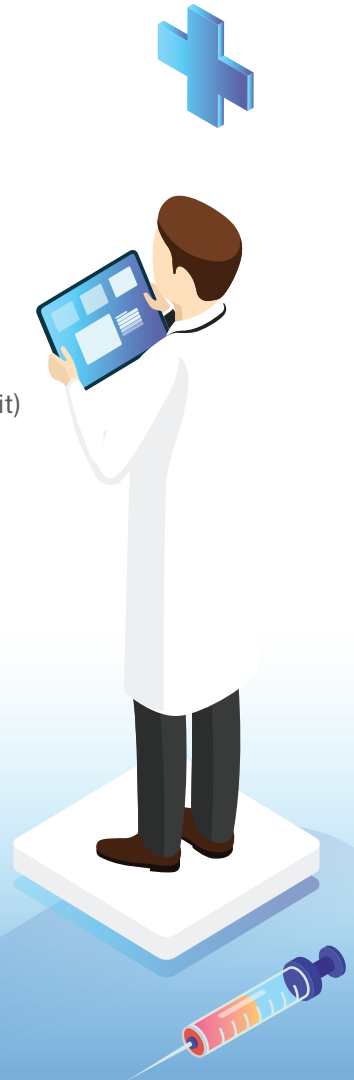


การออกแบบระบบต้นแบบดังกล่าว จะไม่เชื่อมต่อกับระบบบริหารข้อมูล โรงพยาบาล (Hospital Information System: HIS) โดยตรง แต่จะเชื่อมต่อกับฐานข้อมูลเสมือน เพื่อจำลองสถานการณ์การเชื่อมต่อผ่าน Database View ที่โรงพยาบาลสร้างขึ้นไว้บนระบบ Cloud ส่วนตัว สำหรับงานระบบแลกเปลี่ยนข้อมูลสุขภาพโดยเฉพาะ (ซึ่งปัจจุบันติดตั้งอยู่บนระบบ G-Cloud ของ สพร.)

รวมถึงการเชื่อมต่อกับระบบฐานข้อมูล สิทธิประกันสุขภาพที่ได้สมมติขึ้นด้วย ทั้งนี้ ในการจัดทำระบบต้นแบบ e-Referral ได้คำนึงถึงสิทธิในการเป็นเจ้าของข้อมูลของผู้ป่วยเป็นสำคัญ ดังนั้นข้อมูลที่ถูกใช้ในการทดสอบระบบต้นแบบ e-Referral ยกตัวอย่างเช่น ข้อมูลผู้ป่วย ข้อมูลโรงพยาบาล จึงเป็นข้อมูลสมมติเพื่อใช้ในการทดสอบระบบต้นแบบ e-Referral เท่านั้น

ทั้งนี้ในการจัดทำระบบต้นแบบ e-Referral บนเทคโนโลยี Blockchain ได้เลือกโครงสร้างฐานข้อมูลด้านการแพทย์และสุขภาพเพื่อการส่งต่อผู้ป่วย OPD, IPD และ AE/ER สำหรับหน่วยบริการในระบบหลักประกันสุขภาพถ้วนหน้าเขตพื้นที่กรุงเทพมหานคร หรือที่รู้จักกันในชื่อระบบ 13 แฟ้ม มาเป็นมาตรฐานข้อมูลสุขภาพในโครงการนี้ โดยมาตรฐานข้อมูลดังกล่าวประกอบไปด้วยข้อมูลดังต่อไปนี้

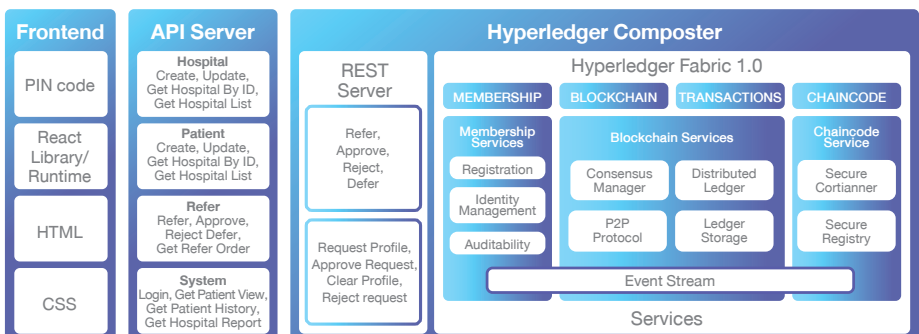
- 🏠 ข้อมูลผู้ป่วย (PID- Patient Identification)
- 🏠 ข้อมูลบุคคลอ้างอิง (NK1- Contact Person)
- 🏠 ข้อมูลการแพ้ (AL1- Patient Allergy)
- 🏠 ข้อมูลการส่งต่อ (RF1- Referral Information)
- 🏠 ข้อมูลการวินิจฉัยโรค (DG1- Diagnosis)
- 🏠 ข้อมูลอาการเจ็บป่วย (Vital Signs)
- 🏠 ข้อมูลการเข้ามารับการรักษา (PV1- Patient Visit)
- 🏠 ข้อมูลทำหัตถการและผ่าตัด (PR1- Procedure)
- 🏠 ข้อมูลผลการตรวจทางห้องปฏิบัติการ (OBL- Observation LAB Result)
- 🏠 ข้อมูลผลตรวจจากภาพถ่ายทางการแพทย์ (OXB- Observation X-Ray Result)
- 🏠 ข้อมูลยาและเวชภัณฑ์ (RXO- Pharmacy/ Treatment Order)
- 🏠 ข้อมูลผู้ให้บริการ (PRD- Provider Data)
- 🏠 ข้อมูลการนัดหมายต่อเนื่อง (APP- Appointment Information)



โดยเลือกใช้ Hyperledger Fabric เวอร์ชัน 1.0 ซึ่งเป็น Open Source ในการพัฒนาระบบต้นแบบดังกล่าว โดย Hyperledger Fabric คือ Blockchain Platform ซึ่งถูกพัฒนาขึ้นภายใต้โครงการ Hyperledger ของ Linux Foundation และเป็นเทคโนโลยี Blockchain ประเภท Private หรือ Permissioned Blockchain ที่มีสถาปัตยกรรมแบบ Modular และสามารถเขียน Smart Contract เพื่อให้ทำงานตามเงื่อนไขได้ โดยบรรจุขั้นตอนการตรวจสอบต่าง ๆ ยกตัวอย่างเช่น การเรียกดูข้อมูลผู้ป่วย ประวัติการรักษา การนัดหมาย รวมถึงข้อมูลที่จำเป็นสำหรับการส่งต่อผู้ป่วยของโรงพยาบาลที่เกี่ยวข้อง โดยใช้ Smart Contract ในการควบคุมขั้นตอน











การตรวจสอบต่าง ๆ ซึ่งใช้ Chaincode เป็นเครื่องมือในการจัดทำ Smart Contract ทั้งนี้ในการพัฒนาระบบต้นแบบดังกล่าว ได้นำเอา Business Logic มาเป็นเงื่อนไขในการสร้าง Smart Contract และ Deploy ลง Hyperledger Fabric ผ่าน Composer และสร้าง API ด้วย REST Sever ของ Composer เพื่อเป็นส่วนติดต่อกับระบบ ดังแสดงในรูปภาพที่ 27



รูปภาพที่ 32: รายละเอียดการออกแบบระบบต้นแบบ e-Referral บนเทคโนโลยี Blockchain

ทั้งนี้ REST Server ของ Hyperledger Composer จะสร้าง REST API ขึ้นมาให้อัตโนมัติจาก Composer Model ซึ่ง API ของระบบต้นแบบ e-Referral บน REST Sever ประกอบไปด้วย 8 API ดังต่อไปนี้

-  **Refer:** ใช้เพื่อเริ่มการขอส่งต่อผู้ป่วย
-  **Approve:** รับการส่งต่อผู้ป่วย
-  **Reject:** ปฏิเสธการส่งต่อผู้ป่วย
-  **CancelReject:** ยกเลิกการปฏิเสธการส่งต่อ
-  **Defer:** ขอเลื่อนเวลาส่งต่อ
-  **RequestProfile:** ขอข้อมูลผู้ป่วย
-  **ApproveRequest:** ผู้ป่วยเจ้าของข้อมูลอนุญาตให้ดูข้อมูลของตนเอง
-  **ClearProfile:** ปิดการเข้าถึงข้อมูลเมื่อหมดเวลาที่อนุญาตให้เข้าดูข้อมูล





แต่เนื่องจาก API บน REST Server ที่ถูกสร้างโดยอัตโนมัติจาก Hyperledger Composer นั้นเป็น API ทั้งหมดของระบบดังได้กล่าวมาแล้วข้างต้น ซึ่งหลายตัวเป็น API ที่ไม่ต้องการเปิดให้ระบบภายนอกเรียกใช้ หรือมี Data Format ที่เข้าใจยากสำหรับผู้ที่ไม่มีส่วนเกี่ยวข้องกับระบบ Blockchain ดังนั้นการพัฒนาระบบต้นแบบ e-Referral ด้วยเทคโนโลยี Blockchain จึงสร้าง API Server ขึ้นมาเป็น Middle Tier โดยทำหน้าที่เป็นจุดเชื่อมต่อ API สำหรับการเรียกใช้งาน ซึ่งประกอบไปด้วย 5 API ดังต่อไปนี้

Hospital: API เกี่ยวกับโรงพยาบาล

End point: /v1/api/hospital
 Method: POST Create Hospital
 PUT Update Hospital
 GET Get Hospital List
 GET Get Hospital By ID
 DEL Delete Hospital

Patient: API เกี่ยวกับผู้ป่วย

End point: /v1/api/patient
 Method: POST Create Patient
 PUT Update Patient
 GET Get Patient List
 GET Get Patient By ID
 DEL Delete Patient



Transaction: API

เกี่ยวกับการส่งต่อผู้ป่วย

End point: /v1/api/transaction/refer

Method: GET Get Refer

POST Refer

POST Approve

GET Get Refer Order

POST Cancel Reject

POST Reject

POST Defer



End point: /v1/api/queries/
selectpatient/

Method: GET Select Patient

GET Select Refer Order

GET Select Refer Order copy

Other

Method: POST Login

GET Get Refer Incoming List

GET Get Refer Outgoing List

POST Hospital Refer

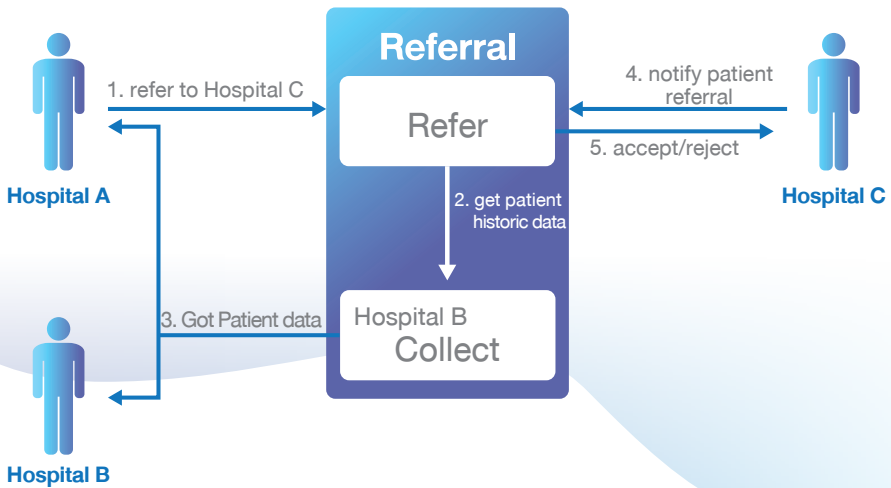
GET Get Patient View



ในส่วนสุดท้ายของการออกแบบระบบต้นแบบ e-Referral คือ การพัฒนาส่วนของ Front End เพื่อใช้โต้ตอบกับผู้ใช้งาน โดยการพัฒนาในส่วนดังกล่าวใช้ ReactJS เป็น Framework และ Cascading Style Sheet หรือ CSS ในการจัดรูปแบบการแสดงผลของเอกสาร HTML



โดยในลำดับถัดไปเป็นการแสดงตัวอย่างเพียงบางส่วนของ ขั้นตอนการส่งต่อผู้ป่วยระหว่างโรงพยาบาล โดยใช้เทคโนโลยี Blockchain ดังแสดงในรูปภาพที่ 28



รูปภาพที่ 33: แผนภาพแสดงขั้นตอนการส่งต่อผู้ป่วยระหว่างโรงพยาบาล



การส่งต่อผู้ป่วยระหว่างโรงพยาบาล ซึ่งในกรณีนี้จะเกิดขึ้นจากการประเมินของแพทย์จำเป็นต้องส่งต่อการรักษาโดยส่งให้เจ้าหน้าที่ของโรงพยาบาลปฐมภูมิ (โรงพยาบาล A) เป็นผู้ศึยข้อมูลการส่งต่อผู้ป่วยให้โรงพยาบาลที่มีความพร้อมมากกว่า เริ่มจากเจ้าหน้าที่ของโรงพยาบาล A เข้าใช้ระบบ e-Referral จาก Username Password ของโรงพยาบาล A เพื่อเข้าสู่หน้าจอการดำเนินงานซึ่งเทียบได้กับ Wallet ของ Blockchain และได้รับ Public Key และ Private Key เพื่อใช้สำหรับการเข้ารหัสรายการธุรกรรม โดยรายการธุรกรรมดังกล่าว คือ การขอส่งต่อผู้ป่วย เมื่อเจ้าหน้าที่ของโรงพยาบาล A กดปุ่มเพื่อส่งรายการขอส่งต่อผู้ป่วยไปยัง

โรงพยาบาลทุติยภูมิ (โรงพยาบาล C) ระบบ e-Referral จะทำการส่งรายการขอส่งต่อผู้ป่วยซึ่งถูกเข้ารหัสด้วย Public Key พร้อม Smart Contract ว่าด้วยข้อกำหนดต่าง ๆ เกี่ยวกับการส่งต่อผู้ป่วย ไปยัง Node อื่น ๆ บนเครือข่าย Blockchain ของระบบ e-Referral และในกรณีที่โรงพยาบาล C ตอบรับการส่งต่อเพื่อรับเข้าเป็นผู้ป่วยของโรงพยาบาล C ดังนั้นโรงพยาบาล C จะสามารถเรียกดูประวัติการรักษาพยาบาลของผู้ป่วยที่เคยเข้ารับการรักษาพยาบาลจากโรงพยาบาลอื่น ๆ ที่อยู่ในเครือข่าย Blockchain ของระบบ e-Referral ได้จากข้อกำหนดที่เขียนไว้ใน Smart Contract ว่าด้วยเรื่องข้อกำหนดในการส่งต่อผู้ป่วย

ในลำดับถัดไปเป็นการแสดงตัวอย่าง
หน้าจอการทำงานเพียงบางส่วนของระบบ
e-Referral



ตัวอย่างที่ 1 การบริหารสิทธิในการเข้าถึงและใช้งานข้อมูลผู้ป่วย โดยใช้ Smart Contract

โรงพยาบาลต้นทางสามารถส่งต่อผู้ป่วยผ่านหน้าจอระบบ e-Referral

```
function requestProfile(req) {
  console.log(req);
  console.log("time stamp : " + req.timestamp.getTime());
  var NS = 'org.acme.blockmd';
  var id = Math.random().toString(36).substring(7)

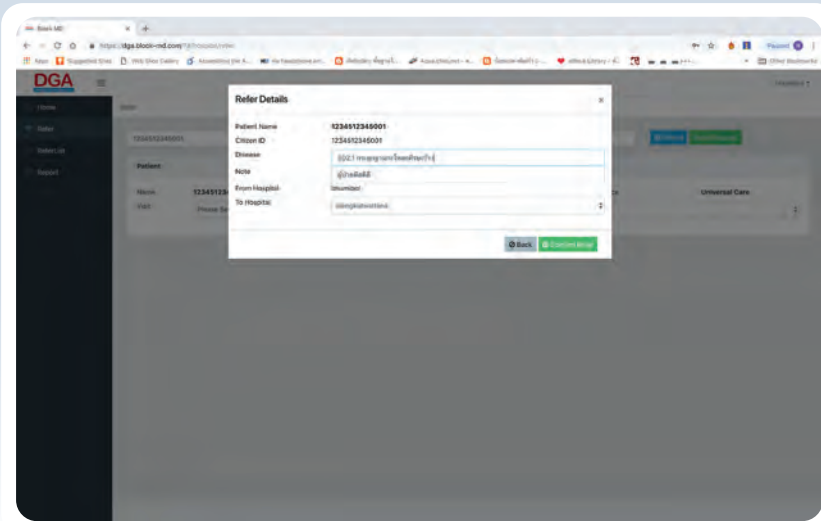
  var profile = getFactory().newResource(NS, 'Profile','' + id);

  profile.state = 'REQUEST';
  profile.id = id;
  profile.requestId = req.id;
  profile.targetId = req.targetId;
  profile.name = req.name;
  profile.timeRequest = req.timestamp;
  return getAssetRegistry(NS + '.Profile')
    .then(function (assetRegistry) {
      return assetRegistry.add(profile);
    });
}
```

รูปภาพที่ 34: ตัวอย่างการเขียนโปรแกรมของการบริหารสิทธิในการเข้าถึง
และใช้งานข้อมูลผู้ป่วย โดยใช้ Smart Contract

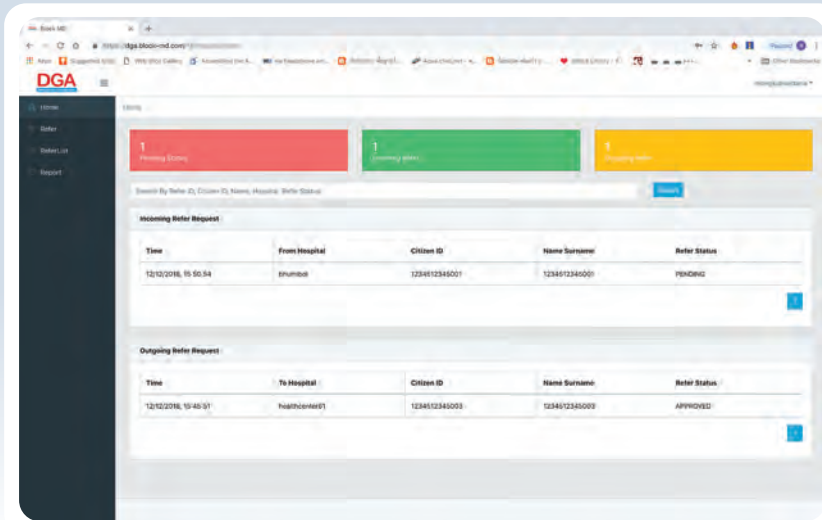
ตัวอย่างที่ 2 ตัวอย่างหน้าจอการส่งต่อข้อมูลผู้ป่วยระหว่างโรงพยาบาลปทุมภูมิ โรงพยาบาลทุติยภูมิ และโรงพยาบาลตติยภูมิ

โรงพยาบาลต้นทางสามารถส่งต่อผู้ป่วยผ่านหน้าจกระบบ e-Referral



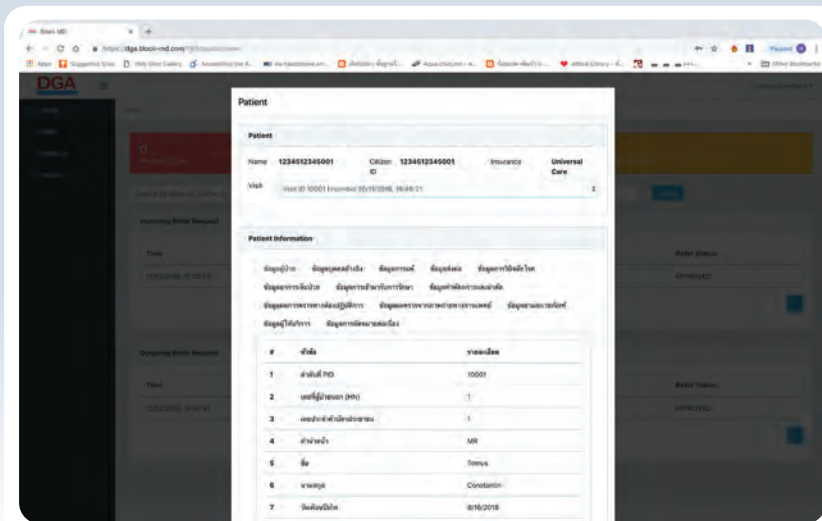
รูปภาพที่ 35: โรงพยาบาลต้นทางสามารถส่งต่อผู้ป่วยผ่านหน้าจกระบบ e-Referral

โรงพยาบาลปลายทางสามารถส่งคำขอส่งต่อผู้ป่วยผ่านหน้าจอระบบ e-Referral



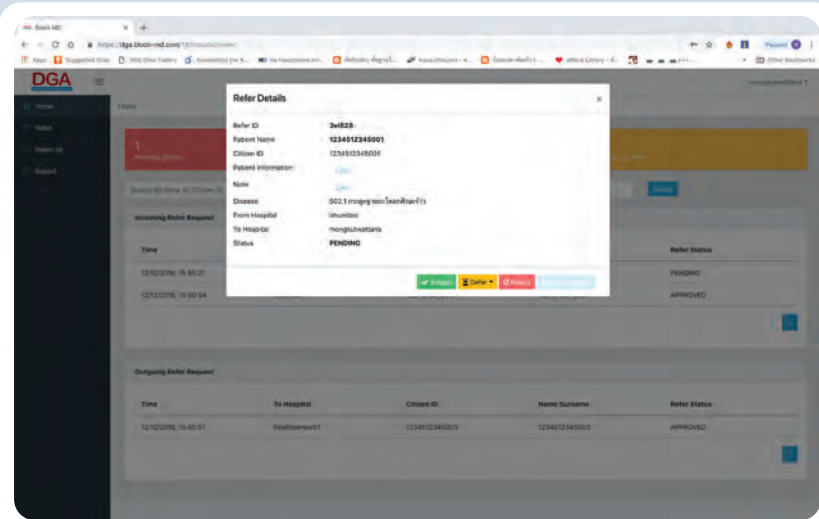
รูปภาพที่ 36: โรงพยาบาลปลายทางสามารถส่งคำขอส่งต่อผู้ป่วยผ่านหน้าจอระบบ e-Referral

โรงพยาบาลปลายทางสามารถเข้าดูข้อมูลผู้ป่วยในระบบ 13 แฟ้มได้



รูปภาพที่ 37: โรงพยาบาลปลายทางสามารถเข้าดูข้อมูลผู้ป่วยในระบบ 13 แฟ้มได้

โรงพยาบาลปลายทางสามารถตอบรับ ปฏิเสธ หรือขอเลื่อนเวลาการส่งต่อผู้ป่วยได้



รูปภาพที่ 38: โรงพยาบาลปลายทางสามารถตอบรับ ปฏิเสธ หรือขอเลื่อนเวลาการส่งต่อผู้ป่วยได้

โรงพยาบาลปลายทางสามารถตอบรับ ปฏิเสธ หรือขอเลื่อนเวลาการส่งต่อผู้ป่วยได้

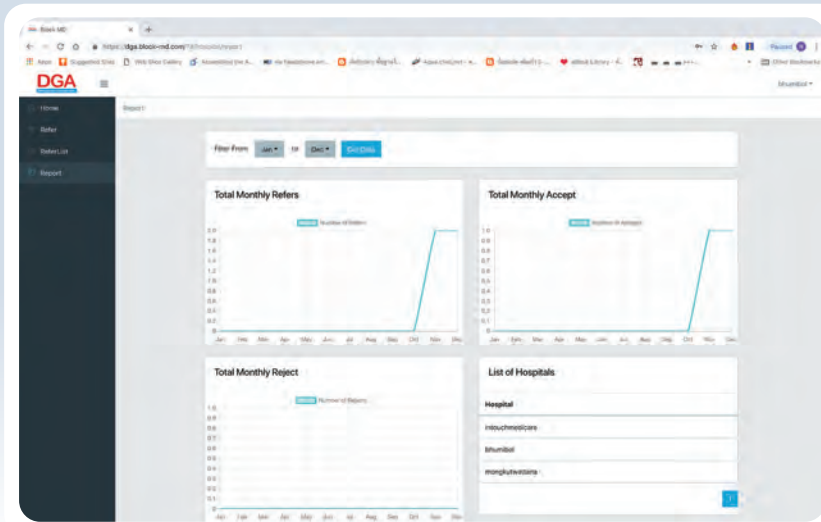
```

{
  "class": "org.hyperledger.composer.system.HistorianRecord",
  "transactionId": "0235ab9bb583e5a817172841768393c913b8f238b110ec1b3ff3afc138221f5e",
  "transactionType": "org.hyperledger.composer.system.UpdateParticipant",
  "transactionInvoked": "resource:org.hyperledger.composer.system.UpdateParticipant#0235ab9bb583e5a817172841768393c913b8f238b110ec1b3ff3afc138221f5e",
  "participantInvoking": "resource:org.acme.blocked.Hospital#201342018343",
  "identityUsed": "resource:org.hyperledger.composer.system.Identity#3568278080dae9a4d43b66e769ec326de6de786fd24d24a823af856c5b8b7491",
  "eventsEmitted": [],
  "transactionTimestamp": "2018-02-19T06:54:01.386Z"
},
{
  "class": "org.hyperledger.composer.system.HistorianRecord",
  "transactionId": "0696ed733124d3167383b67fb25121c8aa65fff761a0b0ffee63a9a13ba17c",
  "transactionType": "org.hyperledger.composer.system.UpdateParticipant",
  "transactionInvoked": "resource:org.hyperledger.composer.system.UpdateParticipant#0696ed733124d3167383b67fb25121c8aa65fff761a0b0ffee63a9a13ba17c",
  "participantInvoking": "resource:org.acme.blocked.Hospital#201342018343",
  "identityUsed": "resource:org.hyperledger.composer.system.Identity#3568278080dae9a4d43b66e769ec326de6de786fd24d24a823af856c5b8b7491",
  "eventsEmitted": [],
  "transactionTimestamp": "2018-02-19T08:12:48.524Z"
}
    
```

รูปภาพที่ 39: ตัวอย่าง Log การส่งต่อผู้ป่วยของระบบ e-Referral

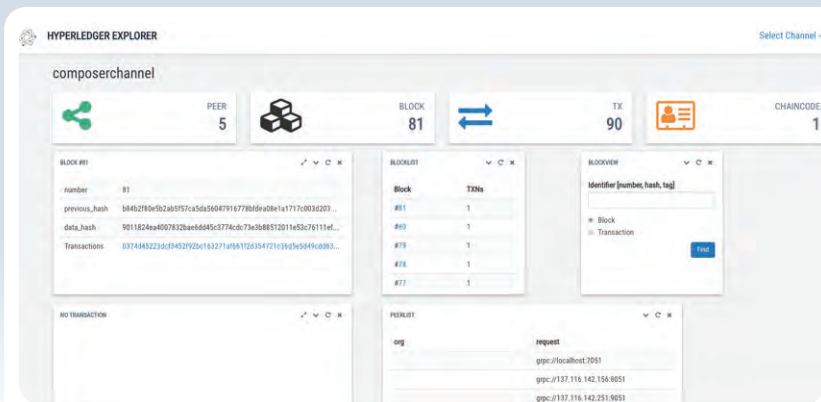
ตัวอย่างที่ 2 ตัวอย่างหน้าจอแสดงรายงาน

หน้าจอ Dashboard แสดงรายงานต่าง ๆ ของระบบ e-Referral



รูปภาพที่ 40: หน้าจอ Dashboard แสดงรายงานต่าง ๆ ของระบบ e-Referral

หน้าจอสำหรับบริการ Performance Monitoring , Report และ Throughput ใน Component ต่าง ๆ ของระบบ Hyperledger Blockchain



รูปภาพที่ 41: หน้าจอสำหรับบริการ Performance Monitoring , Report และ Throughput ใน Component ต่าง ๆ ของระบบ Hyperledger Blockchain

ทั้งนี้ผลจากการศึกษาการพัฒนาระบบต้นแบบ e-Referral พบว่าปัจจัยความสำเร็จในการพัฒนาต่อยอดระบบต้นแบบ e-Referral เพื่อนำไปสู่การยกระดับการให้บริการประชาชน ประกอบด้วย

1

การกำหนดมาตรฐานข้อมูลสุขภาพ Health Data Standard



การกำหนดมาตรฐานข้อมูลสุขภาพ (Health Data Standard) เนื่องจากระบบสุขภาพของไทยได้รับการพัฒนาขึ้นจากหลายหน่วยงาน จึงมีความแตกต่างและหลากหลาย โดยแต่ละระบบจะมีการออกแบบฐานข้อมูลที่มีลักษณะเฉพาะของตนเอง จึงทำให้มีความแตกต่างและหลากหลายของโครงสร้าง ดังนั้นจึงจำเป็นต้องมีการออกแบบมาตรฐานข้อมูลสุขภาพขึ้นมา เพื่อให้สามารถแลกเปลี่ยนข้อมูลได้อย่างมีประสิทธิภาพและใช้ประโยชน์จากการวิเคราะห์ข้อมูลได้



2

การประสานความร่วมมือ Cooperation

การประสานความร่วมมือ (Cooperation) ระหว่างหน่วยงานด้านสาธารณสุขทั้งในภาครัฐและภาคเอกชน ในการเชื่อมต่อกับระบบบริหารจัดการข้อมูลโรงพยาบาล (Hospital Information System: HIS) ยกตัวอย่างเช่น HosXP, HosOS, Trackcare รวมถึงการเชื่อมต่อกับระบบ

หลักประกันสุขภาพ ดังนั้นหากสามารถเชื่อมโยงระบบ e-Referral เข้ากับฐานข้อมูลของระบบเหล่านี้ได้ จะช่วยลดความผิดพลาดจากการกรอกข้อมูลการทำงานที่ซ้ำซ้อน รวมถึงต้นทุนในการทำงาน และเพิ่มประสิทธิภาพในการเชื่อมโยงและแลกเปลี่ยนข้อมูลได้ อีกทั้งยังสามารถทำให้เกิดการใช้ประโยชน์จากข้อมูลทางการแพทย์ในการสร้างนวัตกรรมเพื่อขับเคลื่อนอุตสาหกรรมแพทย์ต่อไปในอนาคตได้

3

โครงสร้างพื้นฐานด้านไอที IT Infrastructure

โครงสร้างพื้นฐานด้านไอที (IT Infrastructure) โครงสร้างพื้นฐานทางไอทีเป็นอีกปัจจัยที่ส่งผลให้การนำระบบ e-Referral บนเทคโนโลยี Blockchain มาใช้งานได้อย่างมีประสิทธิภาพ โดยโครงสร้างพื้นฐานที่เกี่ยวข้องสามารถจำแนกออกได้เป็น 3 กลุ่มด้วยกัน ดังต่อไปนี้



ส่วนต่อเชื่อมกับระบบไอที ของโรงพยาบาล Hospital Interface

เนื่องจากระบบ e-Referral ต้องอ้างอิงข้อมูลจากฐานข้อมูลต่าง ๆ ของโรงพยาบาล ดังนั้นส่วนต่อเชื่อมกับระบบไอทีของโรงพยาบาลจึงเป็นโครงสร้างพื้นฐานหลักที่สำคัญ เพื่อให้ระบบสามารถแลกเปลี่ยนข้อมูลได้แบบ Real-Time และมีความถูกต้อง

อุปกรณ์จัดเก็บข้อมูล Storage

เป็นอุปกรณ์พื้นฐานที่จำเป็นสำหรับเทคโนโลยี Blockchain โดยทำหน้าที่ในการเก็บข้อมูลร่วมกัน รวมถึงเก็บข้อมูลที่มีมูลค่า ยกตัวอย่างเช่น ข้อมูลสุขภาพ ประวัติการเข้ารับการรักษา



ระบบการสื่อสาร

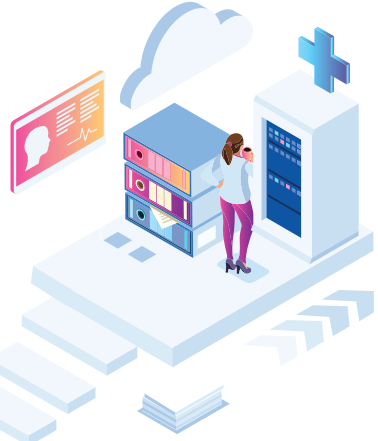
เนื่องจากผู้เข้าร่วมหรือสมาชิกในระบบ Blockchain จำเป็นต้องมีการเชื่อมต่อสื่อสารถึงกันตลอด ดังนั้นระบบการสื่อสารจึงเป็นโครงสร้างที่สำคัญเพื่อให้เกิดการสื่อสารกันภายในเครือข่าย ยกตัวอย่างเช่น การส่งข้อมูลสถานะทั่วไป การยืนยันตัวตนผู้เข้าร่วมระบบ ไปจนถึงข้อมูลการถ่ายโอนสินทรัพย์ที่มีมูลค่าภายในเครือข่าย

เนื่องจากเทคโนโลยี Blockchain มีลักษณะเป็นโครงสร้างแบบกระจาย (Distributed Architecture) ดังนั้นหน่วยงานหรือสมาชิกที่เข้ามาร่วมภายในเครือข่าย จำเป็นต้องเตรียมความพร้อมของอุปกรณ์ ทั้งฝั่งองค์กรเอง และระบบการสื่อสาร เพื่อให้ระบบโดยรวมสามารถดำเนินการต่อไปได้อย่างมีประสิทธิภาพ

4

การเตรียมความพร้อมของบุคลากรที่เกี่ยวข้อง Human Resource Management

กำลังคนและศักยภาพของบุคลากรด้านสาธารณสุขทั้งในส่วนของภาครัฐ และภาคเอกชน เป็นอีกปัจจัยสำคัญที่ส่งผลต่อความสำเร็จของการประยุกต์ระบบ e-Referral บนเทคโนโลยี Blockchain โดยสามารถจำแนกกลุ่มของบุคลากรที่เกี่ยวข้องตามการดำเนินงานออกเป็น 4 กลุ่ม ดังต่อไปนี้



ผู้ดูแลระบบ System Administrators



ผู้บริหารระดับสูงในอุตสาหกรรม สาธารณสุข

มีหน้าที่ในการวางแผนยุทธศาสตร์เพื่อรองรับการใช้งานเทคโนโลยี วางนโยบาย และกฎระเบียบต่าง ๆ ในการดำเนินการสั่งการ มอบหมายงาน และประเมินผลการทำงานแก่ผู้ที่เกี่ยวข้อง

มีหน้าที่ในการดูแลระบบ กิจกรรมภายในระบบ การสื่อสารของระบบให้สามารถดำเนินการได้ปกติ รวมทั้งทำหน้าที่ในการนำระบบขึ้นใช้งาน (Deployment) การต่อเชื่อม และการปรับตั้งค่า (Configuration) ระบบของหน่วยงานให้เชื่อมต่อกับระบบ e-Referral ได้อย่างมีประสิทธิภาพสูงสุด



เจ้าหน้าที่ตรวจสอบ Auditors

มีหน้าที่ในการตรวจสอบการทำงานของระบบ ว่ามีความถูกต้องเหมาะสมตามข้อตกลงที่กำหนดหรือไม่ เริ่มตั้งแต่การตรวจสอบธุรกรรมที่เกิดขึ้นภายในระบบ สิทธิการเข้าถึงของผู้มีส่วนเกี่ยวข้องทั้งหมด รวมถึงตรวจสอบความเที่ยงตรง (Integrity) ของธุรกรรมที่เกิดขึ้นและบัญชีที่จัดเก็บ เพื่อให้สอดคล้องกับกฎระเบียบที่มีการกำหนดขึ้น



เจ้าหน้าที่ปฏิบัติการ System Operators

มีหน้าที่ในการดูแล ตรวจสอบการทำงานของระบบ (Monitoring) เพื่อให้การเชื่อมต่อระหว่างระบบ e-Referral และ Application ที่เกี่ยวข้องสามารถทำงานได้อย่างปกติ และต่อเนื่อง



โอกาสแบบท้าย 1

ตารางสรุปตัวอย่างการประยุกต์ใช้เทคโนโลยี Blockchain สำหรับงานบริการภาครัฐในต่างประเทศ

ประเทศ	โครงการ	สถานะโครงการ	อ้างอิง
ประเทศไทย	บริการหนังสือค้ำประกันอิเล็กทรอนิกส์หรือ e-LG ผ่านเทคโนโลยีบล็อกเชน	โดยใช้งานจริงแล้ว ตั้งแต่ปี ค.ศ.2019	https://www.cgd.go.th , https://www.bci.network
ประเทศออสเตรเลีย	วุฒิสมาชิกประเทศออสเตรเลียได้มีการจัดตั้งคณะทำงานขึ้น เพื่อทำหน้าที่ขับเคลื่อนการนำเทคโนโลยี Blockchain มาใช้ในประเทศออสเตรเลียทั้งภาครัฐและภาคเอกชน	ประกาศในปี 2017	(Martinovic, Kello, & Sluganovic, 2017)
	ตลาดหลักทรัพย์ออสเตรเลีย (ASX) ได้ประกาศจะนำเทคโนโลยี Blockchain มาใช้เพื่อแทนที่ระบบการหักบัญชี และการชำระบัญชีปัจจุบัน ซึ่งก็คือระบบ CHESS (The Clearing House Electronic Sub- Register System)	ประกาศในปี 2017 และเริ่มใช้จริงในปี 2018	(Martinovic et al., 2017)
ประเทศจีน	ระบบบริหารจัดการกองทุนประกันสังคม โดยใช้เทคโนโลยี Blockchain (Social Security Funds Management System)	ประกาศในปี 2016	(Martinovic et al., 2017)
	การประเมินมูลค่าสินเชื่ที่อยู่อาศัย โดยใช้เทคโนโลยี Blockchain (Mortgage Valuations on Blockchain)	ประกาศในปี 2016	(Martinovic et al., 2017)
	ระบบการบริหารจัดการสินทรัพย์ โดยใช้เทคโนโลยี Blockchain (Blockchain-Based Asset Custody System (PSBC))	ประสบความสำเร็จในการใช้งาน โดยใช้งานจริงตั้งแต่ปี 2016	(Martinovic et al., 2017)

ประเทศ	โครงการ	สถานะโครงการ	อ้างอิง
	การพัฒนาโครงการเมืองนวัตกรรมด้านพลังงาน (The Smart City Project of Energy Innovation) โดยใช้เทคโนโลยี Blockchain ร่วมกับเทคโนโลยีด้านอื่น ๆ ยกตัวอย่างเช่น Cloud Computing, Big Data, IoT และ AI ชั้นที่เมือง Hangzhou	ประกาศในปี 2016	(Buterin, Mccaleb, Shen, & Bai, 2018)
	ระบบการจัดเก็บภาษี (Intelligent Tax System) โดยทำงานร่วมกับระบบใบแจ้งหนี้อิเล็กทรอนิกส์ (Electronic Invoice System) ซึ่งทำงานอยู่บนเทคโนโลยี Blockchain เพื่อป้องกันการหลีกเลี่ยงภาษี โดยใช้เอกสารใบแจ้งหนี้ปลอม	ประกาศในปี 2018	(Sundararajan, 2018)
	ระบบการตรวจสอบความปลอดภัยของอาหารทั้งห่วงโซ่อุปทาน (Food Supply Chain Traceability System) โดยใช้เทคโนโลยี Blockchain	ประกาศในปี 2016	(Mao, Wang, Hao, & Li, 2018)
นครรัฐคูโบ ประเทศสหรัฐอาหรับเอมิเรต	ระบบบริหารจัดการข้อมูลและเอกสารภาครัฐ (Government Documents Management System)	อยู่ระหว่างดำเนินการ	(Martinovic et al., 2017)
	หนังสือเดินทางอิเล็กทรอนิกส์ (Digital Passport) โดยใช้เทคโนโลยี Blockchain	ประกาศในปี 2017	(Martinovic et al., 2017)
	ระบบข้อมูลการขนส่งสินค้าแบบเรียลไทม์ (Real-time Shipment Information System)	ประกาศในปี 2017	(Martinovic et al., 2017)
	ระบบจัดเก็บและส่งต่อข้อมูลประวัติการรักษาพยาบาลของผู้ป่วย (Electronic Health Record System: EHRs)	ประกาศในปี 2017	(Kong, 2018)

ประเทศ	โครงการ	สถานะโครงการ	อ้างอิง
	ระบบการออกใบรับรองเพชร (Diamond Certificate) โดย The Dubai Multi Commodities Centre ได้นำเทคโนโลยี Blockchain เข้ามาใช้ในการออกใบ Certificate ให้กับเพชรหรือที่รู้จักกันในชื่อ “Kimberley Certificates”	ประกาศในปี 2017	(Ngo, 2017)
	การจดทะเบียนถือครองกรรมสิทธิ์ที่ดิน (Land Title Registry) ภายใต้ชื่อโครงการ “Dubai Real-Estate Blockchain”	ประกาศในปี 2017	(Journo, 2018)
ประเทศเอสโตเนีย	eID (electronic ID management system)	ใช้งานจริงแล้ว ปัจจุบันอยู่ระหว่างการอัปเดตเวอร์ชัน	(Shen, 2016)
	ระบบบริหารจัดการข้อมูลสุขภาพ หรือ e-Health (Medical Information Management System)	ใช้งานจริงแล้ว ปัจจุบันอยู่ระหว่างการอัปเดตเวอร์ชัน	(Basu, 2018)
	ระบบเอกลักษณ์ดิจิทัลข้ามชาติ หรือ e-Residency (A First-of-a-Kind A Transnational Digital Identity)	ใช้งานจริงแล้ว ตั้งแต่ปี 2015	(Sullivan & Burger, 2017)
	ระบบศาลดิจิทัล (Digital Court System: e-Court) โดยใช้เทคโนโลยี KSI Blockchain มาช่วยในเรื่องของการป้องกันการปลอมแปลงเอกสาร หรือที่เรียกว่าระบบ e-File	ใช้งานจริงแล้ว ตั้งแต่ปี 2015	(Jun, 2018)
	ระบบ Document Registries ต่าง ๆ เช่น Business Registry, Property Registry, Succession Registry และ Healthcare Registry	ใช้งานจริงแล้ว ตั้งแต่ปี 2015	(Martinovic et al., 2017)



ประเทศ	โครงการ	สถานะโครงการ	อ้างอิง
	ระบบการลงคะแนนเสียงเลือกตั้ง (i-Voting) โดยใช้เทคโนโลยี Blockchain	ใช้งานจริงแล้ว ตั้งแต่ปี 2015	(Electronic Voting Committee, 2016)
ประเทศฝรั่งเศส	ระบบการการซื้อขายหลักทรัพย์ที่ไม่ใช่หลักทรัพย์จดทะเบียน	ประกาศในปี 2017	(Martinovic et al., 2017)
ประเทศกานา	การจดทะเบียนถือกรรมสิทธิ์ที่ดิน (Land Title Registry) โดย NGO “Bitland”	อยู่ระหว่างดำเนินการ	(Aitken, 2016)
ประเทศจอร์เจีย	การจดทะเบียนถือกรรมสิทธิ์ที่ดิน (Land Title Registry)	อยู่ระหว่างดำเนินการ	(Jardine, 2018)
ประเทศฮอนดูรัส	การจดทะเบียนถือกรรมสิทธิ์ที่ดิน (Land Title Registry)	ประกาศในปี 2015 แต่โครงการล้มเหลว	
ประเทศรัสเซีย	ระบบบริหารจัดการข้อมูลและเอกสารภาครัฐ (Government Documents Management System)	ประกาศในปี 2016	(Higgins, 2016)
	ระบบบริหารจัดการข้อมูลสุขภาพ หรือ e-Health (Medical Information Management System)	ประกาศในปี 2017	(Jun, 2018)
ประเทศสิงคโปร์	ระบบการชำระเงินระหว่างธนาคารข้ามพรมแดน (Cross-Border Interbank Payments)	ประกาศในปี 2016 และอยู่ระหว่างการทำ Proof-of-Concept	(Jun, 2018)
	ระบบการออกตราสาร การชำระและแลกเปลี่ยนเงินตราและหลักทรัพย์ระหว่างธนาคาร และทดลองใช้งานเงินสกุลแห่งชาติในรูปแบบ Cryptocurrency	อยู่ระหว่างดำเนินการ	(Jun, 2018)

ประเทศ	โครงการ	สถานะโครงการ	อ้างอิง
ประเทศสวีเดน	ระบบการจดทะเบียนถือครองกรรมสิทธิ์ที่ดิน (Land Title Registry) โดยใช้เทคโนโลยี Blockchain และ Smart Contract	อยู่ระหว่างการพัฒนา ทดสอบระบบ ในปี 2017	(Verhulst & Young, 2018)
ประเทศสวิตเซอร์แลนด์	ระบบการชำระค่าธรรมเนียมโดยใช้เงินสกุลดิจิทัล เช่น Bitcoin	ใช้งานจริงแล้ว ตั้งแต่ปี 2016	(Jun, 2018)
	ระบบการจับเก็บอัตลักษณ์ทางดิจิทัล (Digital Identity) โดยใช้หลักการของ Self-Sovereign Identity บนเทคโนโลยี Blockchain	ประกาศในปี 2017	(Verhulst & Young, 2018)
ประเทศยูเครน	ระบบลงคะแนนเสียงเลือกตั้ง e-Vox (Ethereum Blockchain-Based Election Platform)	ประกาศในปี 2016	(Abouzeid, 2016)
	ระบบการประมูลแบบดิจิทัลโดยใช้เทคโนโลยี Blockchain (Blockchain-Based Auction System)	ประกาศในปี 2016	(Ngo, 2016)
	การจดทะเบียนถือครองกรรมสิทธิ์ที่ดิน (Land Title Registry)	ประกาศในปี 2017	(Graglia & Mellon, 2018)
ประเทศอังกฤษ	ระบบการจ่ายสวัสดิการภาครัฐโดยใช้เทคโนโลยี Blockchain	ประกาศในปี 2016 และประสบความสำเร็จในการทดสอบการใช้งานระบบ	(Hebblethwaite, 2017)
	ระบบการบริการภาครัฐต่าง ๆ โดยใช้เทคโนโลยี Blockchain	ใช้งานจริง ตั้งแต่ปี 2016	(Jun, 2018)
	ระบบการชำระเงินระหว่างธนาคารโดยใช้เทคโนโลยี Blockchain	ประกาศในปี 2017	(Jun, 2018)



ประเทศ	โครงการ	สถานะโครงการ	อ้างอิง
ประเทศสหรัฐอเมริกา	ระบบการแลกเปลี่ยนข้อมูลด้านสุขภาพ	ประกาศในปี 2016 และอยู่ระหว่างการทดสอบระบบซึ่งเป็นโครงการนำร่อง	(Jun, 2018)
	อนุญาตให้สามารถทำการซื้อขายหุ้น Bitcoin	ประกาศในปี 2015	(Jun, 2018)
	อนุญาตให้ Blockchain Smart Contract มีผลบังคับใช้ได้ทางกฎหมาย	ประกาศเป็นกฎหมายแห่งรัฐอริโซนา และมีผลบังคับใช้ในปี 2017	(De, 2018)
	อนุญาตให้ใช้เทคโนโลยี Blockchain กับตลาดหลักทรัพย์ในการซื้อขายหุ้นและจัดเก็บข้อมูลธุรกรรมต่าง ๆ ได้และถูกต้องตามกฎหมาย	ประกาศเป็นกฎหมายแห่งรัฐเดลาแวร์ และมีผลบังคับใช้ในปี 2017	(Jun, 2018)
	ระบบ Identity Management บนเทคโนโลยี Blockchain มาใช้ในการเก็บสูติบัตรของเด็กทารกแรกเกิด (Birth Registration) ของรัฐอิลลินอยส์	ประกาศในปี 2017	(Verhulst & Young, 2018)
ประเทศไต้หวัน	ระบบการพิสูจน์และยืนยันตัวตนทางอิเล็กทรอนิกส์ (Citizen Identification)	อยู่ระหว่างการพัฒนา	(Rueter, 2018)
ประเทศญี่ปุ่น	อนุญาตให้ Bitcoin และ Cryptocurrency สามารถใช้ชำระหนี้ได้ตามกฎหมาย	ประกาศในปี 2016	
ประเทศยิบรอลตาร์	อนุญาตให้ใช้เทคโนโลยี Blockchain กับตลาดหลักทรัพย์ในการซื้อขายหุ้นและจัดเก็บข้อมูลธุรกรรมต่าง ๆ ได้และถูกต้องตามกฎหมาย	ประกาศในปี 2017	(Khatri, 2018)

ประเทศ	โครงการ	สถานะโครงการ	อ้างอิง
ประเทศบราซิล	การจดทะเบียนถือครองกรรมสิทธิ์ที่ดิน (Land Title Registry)	ประกาศในปี 2016	(Graglia & Mellon, 2018)
ประเทศ เซียร์ราลีโอน	ระบบการลงคะแนนเสียงเลือกตั้งโดยใช้เทคโนโลยี Blockchain	ประกาศในปี 2018 และอยู่ระหว่างการทำ Proof-of-Concept	(Verhulst & Young, 2018)
ประเทศอินเดีย	การจดทะเบียนถือครองกรรมสิทธิ์ที่ดิน (Land Title Registry)	ประกาศในปี 2017	(Graglia & Mellon, 2018)

Abouzeid, N. (2016). *Ukraine Government Plans to Trial Ethereum Blockchain-Based Election Platform*. Retrieved from <https://bitcoinmagazine.com/articles/ukraine-government-plans-to-trial-ethereum-blockchain-based-election-platform-1455641691/>

Aitken, R. (2016). *Bitland's African Blockchain Initiative Putting Land on The Ledger*. Retrieved from <https://www.forbes.com/sites/rogeraitken/2016/04/05/bitlands-african-blockchain-initiative-putting-land-on-the-ledger/#2f7b8c007537>

Baran, P. (1964). *On distributed communications: I. Introduction to distributed communications networks*. Retrieved from

Basu, M. (2018). *Estonia Using Blockchain to Secure Health Records: Blockchain's Public Sector Use Goes Beyond Payments*. Retrieved from <https://govinsider.asia/innovation/estonia-using-blockchain-to-secure-health-records/>

Belinky, M., Rennick, E., & Veitch, A. (2015). *The Fintech 2.0 Paper: Rebooting Financial Services*. In: Santander InnoVentures.

Breene, K. (2016). *The 10 Countries Best Prepared for the New Digital Economy*. Retrieved from <https://www.weforum.org/agenda/2016/07/countries-best-prepared-for-the-new-digital-economy/>

Buterin, V. (2014). *A next-generation smart contract and decentralized application platform*. white paper.

Buterin, V., Mccaleb, J., Shen, B., & Bai, S. (2018). *Wanxiang Smart City Global Blockchain Challenge*. Retrieved from http://www.wblockchain.com/global/index_en.html

Chase, K. (2017). *Japan Plans Blockchain Test for Government Procurement Process*. Retrieved from <https://dcebrief.com/japan-plans-blockchain-test-for-government-procurement-process/>

Cheng, S., Daub, M., Domeyer, A., & Lundqvist, M. (2017). *Using Blockchain to Improve Data Management in The Public Sector*. Retrieved from <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector>

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). *Blockchain Technology: Beyond Bitcoin*. Applied Innovation, 2, 6-10.

De, N. (2018). *Arizona's Governor Signs Latest Blockchain Bill Into Law*. Retrieved from <https://www.coindesk.com/arizonas-governor-signs-latest-blockchain-bill-into-law>

Deloitte. (2018). *Blockchain in Public Sector: Transforming Government Services through Exponential Technologies*. In (pp. 1-28). India: Deloitte Tohmatsu Limited.

Electronic Voting Committee. (2016). **General Framework of Electronic Voting and Implementation Thereof at National Elections in Estonia**. Tallin University of Technology, 1-21.

Futter, D., Hale, A., Elverston, N., & Waters, T. (2017). **Blockchain 101: An introductory Guide to Blockchain**. Retrieved from <https://www.ashurst.com/en/news-and-insights/insights/blockchain-101/>

Graglia, J. M., & Mellon, C. (2018). **Blockchain and Property in 2018: At The End of The Beginning**. Paper presented at the 2018 World Bank Conference on Land and Poverty Washington DC.

Hebblethwaite, C. (2017). **GovCoin Aims to Disrupt UK Welfare System**. Retrieved from <https://www.blockchaintechnology-news.com/2017/11/28/govcoin-aims-disrupt-uk-welfare-system/>

Higgins, S. (2016). **The Russian Government is Testing Blockchain for Document Storage**. Retrieved from <https://www.coindesk.com/the-russian-government-is-testing-blockchain-for-document-storage>

Holgate, R. (2018). **Blockchain for Government State of Washington**. Retrieved from

Jamsrandorj, U. (2017). **Decentralized Access Control Using Blockchain (Master Degree)**, University of Saskatchewan Saskatoon,

Jardine, B. (2018). ***Georgia Stakes Place on Wild Frontier of Blockchain Governance***. Retrieved from <https://eurasianet.org/georgia-stakes-place-on-wild-frontier-of-blockchain-governance>

Journo, A. H. (2018). ***Dubai Developments will be Built on Blockchain***. Retrieved from <https://digit.fyi/dubai-blockchain/>

Jun, M. (2018). ***Blockchain Government-A Next form of Infrastructure for The Twenty-First Century***. Journal of Open Innovation: Tecnology, Market, and Complexity, 4(7), 1-12. doi:<http://dx.doi.org/10.1186/s40852-018-0086-3>

Khatri, Y. (2018). ***Gibraltar Stock Exchange Wins License for Blockchain Subsidiary***. Retrieved from <https://www.coindesk.com/gibraltar-stock-exchange-wins-license-for-blockchain-subsidiary>

Kohut, I. (2018). ***How Companies Can Leverage Private Blockchains to Improve Efficiency and Streamline Business Processes***. Retrieved from <https://perfectial.com/blog/leveraging-private-blockchains/>

Kong, J. (2018). ***Blockchain UAE: Global Healthcare Implications***. Retrieved from <http://www.milliman.com/insight/2018/Blockchain-UAE-Global-healthcare-implications/>

Krawiec, R., Housman, D., White, M., Filipova, M., Quarre, F., Barr, D., . . . Tsai, L. (2016). ***Blockchain: Opportunities for Health Care***. In (pp. 1-16): Deloitte Development LLC.

Mao, D., Wang, F., Hao, Z., & Li, H. (2018). *Credit Evaluation System Based on Blockchain for Multiple Stakeholders in the Food Supply Chain*. International Journal of Environmental Research and Public Health, 15, 1627-1647. doi:<http://dx.doi.org/10.3390/ijerph15081627>

Marchionni, P. (2018). *Next Generation Government Service Bus: The Blockchain Landscape*. SSRN, 1-42. doi:<http://dx.doi.org/10.2139/ssrn.3141749>

Martinovic, I., Kello, L., & Sluganovic, I. (2017). *Blockchains for Governmental Services: Design Principles, Applications, and Case Studies*. Center for Technology and Global Affairs, 1(7), 1-16.

Morris, N. (2018). *ISO Blockchain Standards Planned for 2021*. Retrieved from <https://www.ledgerinsights.com/iso-blockchain-standards/>

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Ngo, D. (2016). *Feature Interview: Lasha Antadze on Ukraine's Blockchain-Powered State Property Auction System*. Retrieved from <https://btcmanager.com/feature-interview-state-property-auction-system/>

Ngo, D. (2017). *Dubai's Global Blockchain Council Combats "Conflict Diamonds" Trading*. Retrieved from <https://bitcoinmagazine.com/articles/dubais-global-blockchain-council-combats-conflict-diamonds-trading/>

Nuuneoi. (2016). ***Blockchain for Geek***. Retrieved from https://nuuneoi.com/blog/blog.php?read_id=901

Parker, L. (2017). ***Procivis sets out to replace government services with blockchain alternatives***. Retrieved from <https://bravenewcoin.com/insights/procivis-sets-out-to-replace-government-services-with-blockchain-alternatives>

Rueter, T. (2018). ***New Distributed Ledger Digital ID Project Faces a Test in Taiwan***. Retrieved from <https://www.secureidnews.com/news-item/new-distributed-ledger-digital-id-project-faces-a-test-in-taiwan/>

Serrano, Ó. L. (2017). ***Is Blockchain Really Immutable?*** Retrieved from <https://www.bbva.com/en/blockchain-really-immutable/>

Shen, J. (2016). ***e-Estonia: The power and Potential of Digital Identity***. Retrieved from <https://blogs.thomsonreuters.com/answeron/e-estonia-power-potential-digital-identity/>

Sullivan, C., & Burger, E. (2017). ***e-Residency and Blockchain***. *Computer Law & Security Review*, 33(4), 470-481. doi:<http://dx.doi.org/10.1016/j.clsr.2017.03.016>

Sundararajan, S. (2018). ***Chinese City to Use Blockchain In Fight Against Tax Evasion***. Retrieved from <https://www.coindesk.com/tencent-partners-with-city-authority-to-combat-tax-evasion-with-blockchain>

Umeh, J. (2016). *Blockchain Double Bubble or Double Trouble?* ITNOW, 58(1), 58-61. doi:<http://dx.doi.org/10.1093/itnow/bww026>

Veedvil. (2017). *ทำความเข้าใจเทคโนโลยี Blockchain จุดเปลี่ยนของหลายอุตสาหกรรม*. Retrieved from <http://www.veedvil.com/news/blockchain/>

Verhulst, S. G., & Young, A. (2018). *Blockchange: Blockchain Technologies for Social Change*. GovLab, 1-98.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018a). *Blockchain Technology Overview*. National Institute of Standards and Technology (NIST), 8202, 1-68. doi:<https://doi.org/10.6028/NIST.IR.8202>

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018b). *Blockchain technology overview*. Draft NISTIR, 8202.

Yermack, D. (2017). *Corporate governance and blockchains*. Review of Finance, 21(1), 7-31.

Zheng, Z., Xie, S., Dai, H.-N., & Wang, H. (2016). *Blockchain challenges and opportunities: A survey*. International Journal of Web and Grid Services, 1, 1-25.

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (2560). *(ร่าง) แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2560-2564*. ประเทศไทย

อาชวานันท์กุล, ส. (2016). *จาก “สัญญาอัจฉริยะ” สู่ “องค์กรอัตโนมัติกระจายศูนย์” (decentralized autonomous organization – DAO)*. Retrieved from <http://thaipublica.org/2016/09/decentralized-autonomous-orgs/>

DGA

Digital Government Development Agency

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Digital Government Development Agency (Public Organization) (DGA)
www.dga.or.th |     [dgathailand](https://www.dgathailand.com)

อาคารบางกอกไทยทาวเวอร์ 108 ถนนรางน้ำ
แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ 10400
โทรศัพท์ : (+66) 0 2612 6000
โทรสาร : (+66) 0 2612 6011 , (+66) 0 2612 6012
Contact Center : (+66) 0 2612 6060
อีเมล : contact@dga.or.th

ดาวน์โหลด e-Magazine ฟรี



 SOY-BASED INKS

This book is printed using
eco - friendly soy inks