การพัฒนากรอบสถาปัตยกรรมการสับเปลี่ยนเอกสารธุรกรรมทางอิเล็กทรอนิกส์ระหว่างหน่วยงานภาครัฐที่มีประสิทธิภาพและความมั่นคงปลอดภัยด้วยเทคโนโลยีบล็อกเชน

Development of Efficient and Secured Electronic Transaction Document Interchange Architecture Framework among Public Sector with Blockchain Technology

ชัยพร ทบแป (Chaiporn Thoppae)*, ประสงค์ ปราณีตพลกรัง (Prasong Praneetpolgrang)**
และ นิเวศ จิระวิชิตชัย (Nivet Jirawichitchai)***

Received : November 4, 2019
Revised : February 5, 2019
Accepted : March 5, 2019

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อพัฒนากรอบสถาปัตยกรรมการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ระหว่างหน่วยงานภาครัฐด้วยเทคโนโลยีบล็อกเชน งานวิจัยนี้เป็นทั้งเชิงคุณภาพและเชิงปริมาณ จากการศึกษานโยบาย และงานวิจัยที่เกี่ยว การสัมภาษณ์เชิงลึกกับผู้เชี่ยวชาญจำนวน 25 คน ผลการสัมภาษณ์เชิงลึก การวิเคราะห์เนื้อหาและออกแบบสถาปัตยกรรมการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ ได้นำไปทดลองใช้ในสำนักงานคณะกรรมการอาหารและยา ทั้งนี้ แนวทางการพัฒนากรอบสถาปัตยกรรมการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์จะต้องให้ความสำคัญกับคุณสมบัติเฉพาะของเทคโนโลยีบล็อกเชนที่สามารถช่วยแก้ปัญหาลดความซับซ้อนของขั้นตอนการทำงาน รวมทั้งความถูกต้องของเครือข่าย การกระจายอำนาจ ความมั่นคงปลอดภัย การมีส่วนร่วม ความโปร่งใส ความไว้วางใจ การเข้าถึงสิทธิ์ และการมีมาตรฐานสากล ผลการวิจัยพบว่า การรับ-ส่งเอกสารร่วมกับเทคนิคการเข้ารหัสแบบสมมาตรของดิฟฟี-เฮล แมน และการใช้ลายมือชื่ออิเล็กทรอนิกส์ร่วมกับบล็อกเชนสามารถแก้ปัญหาการสับเปลี่ยนเอกสารภาครัฐได้อย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัยสูง

คำสำคัญ: บล็อกเชน การสับเปลี่ยนเอกสาร ธุรกรรมอิเล็กทรอนิกส์

Abstract

The objective of this research is to find ways to develop an electronic document exchange architecture among government agencies with efficiency and security based on blockchain technology. This research used both qualitative and quantitative method. By collecting data from the policy, theory, and related works used in-depth interview with 25 experts. Then, we determine the content analysis and design a framework of electronic transaction document interchange architecture. A case study in the food and drug administration (FDA) for the proposed architecture framework. In this regard, guidelines for developing electronic document interchange among public sector must focus on bringing the unique properties of blockchain technology to solve problems in order to reduce the complicated work processes, including network accuracy with decentralization, security and safety, participation, transparent, trust, rights to access, and deal with the international standards. The result of using the architectural design found that document sending and receiving with symmetric encryption technique of Diffie and Hellman to encrypt documents with electronic signature and blockchain technology could solve the problem of electronic transaction document interchange among public sector efficiently and with high security.

Keywords: Blockchain, Document Interchange, Electronic Transaction

* บัณฑิตศึกษา คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
* Graduate School, Faculty of Information Technology, Sripatum University.
** ศาสตราจารย์ บัณฑิตศึกษา คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
** Professor of Graduate School, Faculty of Information Technology, Sripatum University.
*** ผู้ช่วยศาสตราจารย์ บัณฑิตศึกษา คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
*** Assist. Prof. of Graduate School, Faculty of Information Technology, Sripatum University.

1. บทนำ

นับจากอดีตที่ผ่านมาจนถึงปัจจุบันการติดต่อสื่อสารภาคราชการยังมีปัญหาเป็นอย่างมากทั้งการติดต่อประสานงานในหน่วยงานของภาครัฐด้วยกันเอง หรือหน่วยงานภาคเอกชนประสานงานติดต่อกับภาครัฐตลอดจนประชาชนติดต่อกับภาครัฐ ด้วยการทำงานของภาครัฐมีความซับซ้อนและมีขั้นตอนเป็นจำนวนมากผู้ที่มาติดต่อไม่สามารถตรวจติดตามหรือตรวจสอบกระบวนการทำงานได้ว่าตอนนี้อยู่ในกระบวนการใดแล้ว

จะสังเกตเห็นว่า กลไกการสับเปลี่ยนเอกสารสำหรับการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐในโครงการบูรณาการงานบริการภาครัฐเพื่อเพิ่มประสิทธิภาพ และระบบบริการทางอิเล็กทรอนิกส์ภาครัฐแบบเบ็ดเสร็จจากช่องทางเดียว (National Single Window : NSW) ยังขาดการเชื่อมโยงการทำงานภาครัฐให้เสมือนเป็นองค์กรเดียวแบบบูรณาการอย่างแท้จริง หากแต่เป็นเพียงการเชื่อมโยงและสับเปลี่ยนข้อมูลพื้นฐานซึ่งไม่น่าจะเพียงพอและยังขาดหลักการออกแบบที่เป็นสากล ทั้งนี้ เนื่องจากขาดคุณสมบัติที่สำคัญยิ่งอันได้แก่ การหลอมรวมเชื่อมต่อให้เสมือนเป็นองค์กรเดียว ความโปร่งใส ความไว้วางใจ และความมั่นคงปลอดภัย

จากการสำรวจสภาพเทคโนโลยีสารสนเทศที่หน่วยงานภาครัฐใช้อยู่ในปัจจุบันประกอบกับวิเคราะห์เทคโนโลยีดิสรัปชันสมัยใหม่ อาทิ เทคโนโลยีดิจิทัล ผู้วิจัยจึงมีความเห็นว่าหน่วยงานภาครัฐควรต้องมีการนำระบบการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ (Electronic Transaction) มาเพื่ออำนวยความสะดวก เพิ่มความรวดเร็ว ลดเวลา ลดระยะทาง และลดค่าใช้จ่ายในการมาติดต่อกับเจ้าหน้าที่ภาครัฐ ยกระดับการติดตามงาน สร้างความโปร่งใสในการทำงานให้บริการภาครัฐด้วยการบูรณาการงานบริการภาครัฐให้มีประสิทธิภาพ (Thailand Gateway) โดยมี 1. ศูนย์กลางบริการข้อมูล (Information Gateway) 2. ศูนย์กลางบริการด้านการลงทุน (Investment Gateway) 3. ศูนย์กลางบริการด้านการค้า (Trade Gateway) 4. ศูนย์กลางบริการด้านประชาชน (Citizen Gateway) 5. ศูนย์กลางบริการด้านการท่องเที่ยว (Tourist Gateway) และ 6. ระบบสนับสนุนการดำเนินงาน (Support Functions) และควรมีระบบบริการอิเล็กทรอนิกส์ภาครัฐแบบเบ็ดเสร็จจากช่องทางเดียว (National Single Window: NSW) ซึ่งเป็นระบบการบริการเชื่อมโยงข้อมูลหน่วยงานระหว่างหน่วยงานภาครัฐ (G2G) การเชื่อมโยงข้อมูลระหว่างหน่วยงานภาครัฐกับภาคธุรกิจ (G2B) และการเชื่อมโยงข้อมูลระหว่างหน่วยงานภาคธุรกิจและภาคธุรกิจ (B2B) สำหรับการนำเข้า ส่งออกจากรูปแบบระบบโครงสร้างงานดังที่กล่าวมา ระบบทั้งหมดข้างต้นยังเป็นระบบการรวมศูนย์กลาง อีกทั้งรูปแบบของการสับเปลี่ยนเอกสารสำหรับธุรกรรมทางอิเล็กทรอนิกส์ยังมีการเชื่อมต่อกับภาคประชาชน (G2C) ได้อีกด้วย

จากเหตุผลที่กล่าวมาข้างต้น ผู้วิจัยจึงศึกษาเรื่องการพัฒนากรอบสถาปัตยกรรมการสับเปลี่ยนเอกสารเพื่อการทำธุรกรรมทางอิเล็กทรอนิกส์ระหว่างหน่วยงานภาครัฐที่มีประสิทธิภาพและมั่นคงปลอดภัยโดยการใช้เทคโนโลยีบล็อกเชน โดยมีความสอดคล้องตามบริบทของเศรษฐกิจดิจิทัลภายใต้แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

1. แนวคิดพื้นฐานการสับเปลี่ยนเอกสารธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐที่มีประสิทธิภาพและความมั่นคงปลอดภัย คือ การสื่อสารถึงกันได้อย่างรวดเร็วไร้ขอบเขตจำกัด การสับเปลี่ยนข้อมูลอิเล็กทรอนิกส์ (Electronic Data Interchange : EDI) เป็นกลยุทธ์การสื่อสารอีกประเภทหนึ่ง ซึ่งหลายองค์กรได้นำมาใช้ ทำให้การสื่อสารสะดวกรวดเร็ว ประหยัดงบประมาณในเรื่องการใช้กระดาษและการขนส่ง ซึ่งนำไปสู่การลดต้นทุนทางธุรกิจ สอดคล้องตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเห็นความสำคัญของการทำธุรกรรมการสับเปลี่ยนเอกสารอิเล็กทรกนิกส์

2. แนวคิดและหลักพื้นฐานสำคัญของเทคโนโลยีบล็อกเชน ได้แก่

2.1 ความหมายของบล็อกเชน

กรรมการราชบัณฑิตสาขาคอมพิวเตอร์ได้ให้ความหมายของคำว่า “บล็อกเชน” ไว้ว่า วิธีการเก็บข้อมูลรายการเปลี่ยนแปลงตามหลักทางบัญชี โดยการเข้ารหัสและจัดเรียงข้อมูลเหล่านี้ต่อกันตามลำดับเวลาที่ข้อมูลเข้ามา กลุ่มข้อมูลดังกล่าวจะเผยแพร่ไปให้ผู้ใช้ในเครือข่ายที่กำหนดได้ทราบทั่วกันทั้งนี้ผู้ใช้ทุกคนจะทราบการแก้ไขเพิ่มเติมรายการเปลี่ยนแปลงในบล็อกเชนทุกรายการตลอดเวลา

2.2 แนวคิดและหลักการทำงานพื้นฐานสำคัญของบล็อกเชน

ในปี 1970 Ralph Markle [1] ได้นำเสนอ Markle Tree หรือ Hash Tree เป็นการเริ่มพัฒนาบล็อกเชน และได้ทำการจดสิทธิบัตรในปี 1979 ซึ่งประกอบด้วยการสร้าง leaf Node และ Non-leaf Node เป็น Tree Diagram โดยที่ทุก ๆ Leaf Node จะมีค่าบล็อกข้อมูล และในทุก Non-leaf Node จะบันทึกค่า Cryptographic Hash ของค่าบล็อกข้อมูลของ Leaf Node Child ของตัวมันเอง ต่อมาในปี 1991 Stuart Haber และ W. Scott Stornetta [2] เริ่มพัฒนาแนวคิดในการทำบล็อกเชนขึ้นมาก่อน และจากนั้นจึงได้นำเอา Markle Tree มาผสานเข้าไปกับแนวคิดของตนจนกลายเป็น “บล็อกเชน” ต่อมา Nakamoto Satoshi [3] นำไปเป็นพื้นฐานในการสร้าง Cryptocurrency ในปี 2008 และเกิดเป็น Bitcoin ในเวลาต่อมา บล็อกเชนมีการกล่าวถึงกันเป็นอย่างมากว่าเป็นเทคโนโลยีอุบัติใหม่ที่สามารถปฏิวัติโลกหรือพลิกโลกและสร้างความน่าเชื่อถือมากที่สุด ลดการมีคนกลาง สร้างความโปร่งใส โดยหลักการสำคัญของบล็อกเชน มีทั้งหมด 7 ประการ ตามที่ Don และ Alex Tapscott [4] ได้กำหนดไว้ ประกอบด้วย 1. ความถูกต้องของเครือข่าย 2. การกระจายอำนาจ 3. การใช้มูลค่าเป็นสิ่งจูงใจ 4. ความมั่นคงปลอดภัย 5. ความเป็นส่วนตัว 6. การดำรงสิทธิ์ และ 7. การมีส่วนร่วม

2.3 ประเภทของบล็อกเชน

บล็อกเชนสามารถแบ่งออกได้เป็น 3 ประเภท โดยพิจารณาจากข้อกำหนด ในการเข้าร่วมเป็นสมาชิกของเครือข่าย คือ บล็อกเชนแบบเปิดสาธารณะ (Public Blockchain) บล็อกเชนแบบปิด(Private Blockchain และบล็อกเชนแบบเฉพาะกลุ่ม (Consortium Blockchain)

3. นโยบายแนวคิดการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ในประเทศไทย ได้แก่ยุทธศาสตร์ชาติ 20 ปี (2561 – 2580) [5] กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะพ.ศ. 2554-2563 [6] นโยบายและแผนระดับชาติว่าด้วย การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2561-2580) [7] แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 (พ.ศ. 2560-2564) [8] แผนยุทธศาสตร์การพัฒนาระบบโลจิสติกส์ของประเทศไทย ฉบับที่ 3 (พ.ศ. 2560-2564) [9]

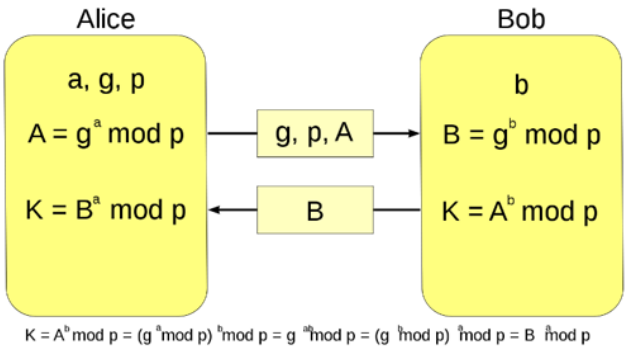
4. แนวคิดและมาตรฐานสากลที่เกี่ยวข้องกับการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ ได้แก่ ด้านการให้บริการ ISO/IEC 20000 [10] ด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001[11], NISt Cybersecurity Framework [12] และด้านการบริหารความเสี่ยง ISO/IEC 27005 [13]

5. ปัจจัยจำเป็นที่มีผลต่อการจัดทำกรอบสถาปัตยกรรมการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ของประเทศไทย ด้านนโยบายด้านกฎหมาย กฎระเบียบที่เกี่ยวข้องปัจจัยด้านสังคม ปัจจัยด้านอรรถศาสตร์ ปัจจัยด้านเทคโนโลยี

6. การจัดการธุรกิจอิเล็กทรอนิกส์ระหว่างหน่วยงานหน่วยงาน เป็นการบริหารจัดการภาครัฐสมัยใหม่ที่เน้นการใช้เทคโนโลยีคอมพิวเตอร์และเครือข่ายเพื่อเพิ่มประสิทธิภาพของผลงานของภาครัฐ และปรับปรุงการบริการแก่ประชาชน โดยการใช้เทคโนโลยีจะนำมาใช้เพื่อเพิ่มศักยภาพของการเข้าถึงและการให้บริการของรัฐ โดยมุ่งเป้าหมายไปที่กลุ่มคน 3 ภาค 4 กลุ่ม คือ ภาคประชาชน (G2C รัฐกับประชาชน) ภาคธุรกิจ (G2B รัฐกับเอกชน) และภาครัฐและข้าราชการ (G2G รัฐกับรัฐ และ G2E รัฐกับข้าราชการและพนักงานของรัฐ)

7. การแลกเปลี่ยนกุญแจแบบดิฟฟี-เฮลแมน

วิธีการแลกเปลี่ยนกุญแจรหัสแบบดิฟฟี-เฮลแมน (Diffie-Hellman) [14] ได้นำมาใช้กับวิทยาการรหัสลับที่ทำให้ผู้รับและส่งไม่จำเป็นต้องมีกุญแจรหัสของทั้งสองฝ่าย แต่สารมารถสร้างกุญแจหัสเพื่อใช้ร่วมกันโดยที่ไม่ต้องส่งกุญแจรหัสไปให้อีกฝ่ายผ่านช่องทางการสื่อสารไม่ปลอดภัย เนื่องจากกุญแจรหัสจะไม่ถูกส่งผ่านช่องทางการสื่อสารเลย ดังนั้น กุญแจรหัสที่ได้จากอัลกอริทึมนี้จึงสามารถนำมาใช้เป็นกุญแจรหัสสำหรับอัลกอริทึม การเข้ารหัสแบบสมมาตร ดังภาพที่ 1



ภาพที่ 1 *การแลกเปลี่ยนกุญแจรหัสแบบดิฟฟี-เฮลแมน*

ในภาพที่ 1 เมื่ออลิสต้องการสร้างกุญแจรหัสในการส่งข้อมูลระหว่างกัน อลิสจะเลือกจำนวนเฉพาะ 2 จำนวน คือ p และ q จากนั้นอลิสจะเลือกจำนวนเต็ม a ขึ้นมาและคำนวณหาค่า A ซึ่งมีค่าเท่ากับ $A = g^a \bmod p$ จากนั้นอลิสจะส่งค่า g, p, A ไปให้กับบ๊อบ ซึ่งเลือกจำนวนเต็ม b เตรียมไว้ก่อนแล้ว เมื่อได้รับค่า g, p, A บ๊อบจะคำนวณหาค่า B ซึ่งมีค่าเท่ากับ $B = g^b \bmod p$ จากค่า g, p ที่ได้รับมาจากอลิส แล้วส่งค่า B ให้กับอลิส อลิสจะคำนวณหาค่ากุญแจรหัสได้จาก $K = B^a \bmod p$ และบ๊อบก็จะคำนวณหาค่ากุญแจรหัสได้จาก $K = A^b \bmod p$ทั้งนี้ในกรณีที่มีผู้แอบดักรับข้อมูลที่รับ-ส่งกันระหว่างอลิสและบ๊อบผู้ที่ดักรับจะไม่สามารถคำนวณหากุญแจรหัสที่สร้างขึ้นมาได้จากวิธีการแบบนี้ทั้งนี้เนื่องจากหากเลือกจำนวนเฉพาะ g อย่างเหมาะสมแล้วการคำนวณหา a และ b แทบจะเป็นไปไม่ได้ แม้ว่าจะใช้เครื่องคอมพิวเตอร์ที่มีประสิทธิภาพสูงก็ตาม กุญแจที่ได้จากวิธีการแลกเปลี่ยนกุญแจรหัสแบบดิฟฟี-เฮลแมน
คำนวณได้จาก

$$\begin{aligned} K &= A^b \bmod p = (g^a \bmod p)^b \bmod p \\ &= g^{ab} \bmod p \\ &= (g^b \bmod p)^a \bmod p \\ &= B^a \bmod p \end{aligned}$$

8. ลายมือชื่ออิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) คือ ชุดข้อมูลตัวอักษร หรือบิตสตริงที่ใช้แสดงความน่าเชื่อถือของเอกสารดิจิทัลที่ถูกลงลายมือชื่อการกระทำใด ๆ ตามรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ ในการสร้างลายมือชื่ออิเล็กทรอนิกส์ ใช้กระบวนการที่เรียกว่า “การเข้ารหัสแบบอสมมาตร (Asymmetric Algorithm)” ซึ่งเป็นกระบวนการที่ทำให้ผู้รับมั่นใจได้ว่าเอกสารที่ได้รับนั้นมาจากผู้ส่งที่แท้จริง การทำงานของลายมือชื่ออิเล็กทรอนิกส์ประกอบด้วย 3 ลักษณะ ได้แก่ การสร้างลายมือชื่ออิเล็กทรอนิกส์ (Signing) การสร้างกุญแจ (Key Generation) และการตรวจสอบลายมือชื่อ (Signature Verifying) [15]

2.4 งานวิจัยที่เกี่ยวข้อง

ผู้วิจัยยังได้ศึกษางานวิจัยที่เกี่ยวข้องการประยุกต์ใช้เทคโนโลยีบล็อกเชนเพื่องานบริการภาครัฐทั้งในและต่างประเทศดังนี้

T. Santhanamerya และ T. Ramayahb ได้ทำการวิจัยโดยศึกษาความต่อเนื่องของความตั้งใจในการใช้ระบบการยื่นคำร้องคำขอหนังสือหรือเอกสารทางอิเล็กทรอนิกส์ (e-Filing) ซึ่งเป็นหนังสือราชการทางออนไลน์ในประเทศมาเลเซียที่ให้บริการแก่ประชาชนมาตั้งแต่ปี พ. ศ. 2549 ในกรณีศึกษานี้เป็นการสำรวจประชาชนใน 5 เมืองใหญ่ของประเทศมาเลเซียที่มีต่อระบบการจ่ายภาษี ในงานวิจัยพบว่ามีความสัมพันธ์ในระดับมากระหว่างความตั้งใจในการใช้ระบบการยื่นคำร้องทางอิเล็กทรอนิกส์กับความเสี่ยงที่จะเกิดขึ้น อย่างไรก็ดี คณะผู้วิจัยได้นำเสนอแนวทางที่เหมาะสมในการลดความเสี่ยงดังกล่าว [16]

ปีเตอร์ รักธรรม ได้ทำการศึกษาปัจจัยและกลยุทธ์ที่สร้างแรงจูงใจในการใช้ระบบเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ พบว่านอกจากปัจจัยที่เกี่ยวข้องกับตัวระบบ ยังมีปัจจัยอื่น ๆ ที่ไม่เกี่ยวข้องกับคุณลักษณะของระบบ แต่จะช่วยเสริมให้เกิดการใช้งานระบบได้มากขึ้น ซึ่งได้เสนอแนะให้หน่วยงานภาครัฐควรมีการจัดตั้งหน่วยงานกลางที่มีอำนาจในการสั่งการ และติดตามงานเพื่อทำหน้าที่ในการประสานงานของทุกกรม [17]

Tierion กล่าวว่าเทคโนโลยีบล็อกเชนใช้เทคโนโลยีการยืนยันตัวตนหลายขั้นตอน (Multi-Factor Authentication: MFA) และระบบที่ให้ผู้ใช้ทำการยืนยัน ตัวตนอีกครั้ง กรณีมีผู้ใช้คนอื่นเป็นเจ้าของรวมกันจำเป็นต้องได้รับอนุญาตจากเจ้าของร่วมกันด้วย เพื่อทำให้ข้อมูลมีความปลอดภัยสูงและโปร่งใส และจากงานวิจัยได้มีการใช้เทคโนโลยีบล็อกเชนในการปกป้องข้อมูลส่วนตัวและเก็บรักษาข้อมูลของบุคคลและแชร์ข้อมูลส่วนตัวกันโดยไม่อาศัยตัวกลาง เช่น สำนักทะเบียนประชากร เพื่อยืนยันความถูกต้องของข้อมูลโดยทุกคนจะมีบัญชีส่วนตัวที่ใช้การเข้ารหัสข้อมูลแบบบล็อกเชนในการเข้าถึงข้อมูลส่วนตัว และเชื่อมโยงข้อมูลเข้าด้วยกันกับ ข้อมูลของบุคคลอื่น ๆ ในระบบ [18]

W.K.Meijer, D,Middendorp, J.M. Raes และ R. Tubbing ได้วิจัยและพัฒนาระบบ e-Passports โดยใช้ระบบบล็อกเชน

เข้ามาช่วยในการระบุตัวตนและระบุการทำธุรกรรมต่าง ๆ ที่เกิดขึ้นซึ่งมีความน่าเชื่อถือ และตรวจสอบได้ อีกทั้งยังช่วยลดขั้นตอนการทำงานของบุคคลเพื่อใช้ยืนยันตัวตน ทำให้เกิดความรวดเร็วและประหยัดค่าใช้จ่ายได้ [19]

D. A. Wijaya ศึกษาพบว่าธุรกิจต้องการความไว้วางใจในการทำการค้าอย่างมั่นใจระหว่างกัน และรูปแบบการจ่ายศูนย์กลางได้รับความนิยมอย่างมาก และกำลังเป็นที่ยอมรับสำหรับธุรกิจในอนาคต การศึกษานี้ยังได้นำเสนอแนวคิดของการใช้บล็อกเชนออกแบบระบบชำระภาษีมูลค่าเพิ่ม (VAT) ให้เป็นระบบใหม่ของซาอุดิอาระเบียในการแก้ปัญหาการจ่ายภาษีซ้ำซ้อน ป้องกันการคอรัปชัน การทำธุรกรรมที่เกี่ยวข้องกับแต่ละกิจกรรมหรือรายการที่ดำเนินการโดยผู้มีส่วนได้ส่วนเสียมีความโปร่งใส และอัพเดทข้อมูลทั้งหมดให้ฝ่ายที่เกี่ยวข้องพร้อม ๆ กัน [20]

กล่าวโดยสรุปแล้ว เทคโนโลยีบล็อกเชนจะเป็นลำดับของบล็อกหรือกลุ่มระเบียนธุรกรรมที่ในแต่ละกลุ่มระเบียนได้ใช้วิธีการเข้าหัสเพื่อเชื่อมข้อมูลเข้าเป็นกลุ่มระเบียนที่เปลี่ยนรูปไม่ได้ทั้งนี้ในรายละเอียดจะเป็นการแลกเปลี่ยนและกระจายบัญชีธุรกรรมอิเล็กทรอนิกส์กับผู้ที่เกี่ยวข้องในเครือข่ายซึ่งข้อมูลจะถูกบันทึกถาวร เปลี่ยนแปลงไม่ได้ อีกทั้งยังมีกลไกในการป้องกันการแก้ไขรายการข้อมูลจากธุรกรรมใด ๆ ไม่ให้ผิดเพี้ยนไปจากต้นฉบับ ทำให้ระบบคอมพิวเตอร์ในเครือข่ายบล็อกเชนสามารถรักษาความสมบูรณ์ถูกต้องครบถ้วนของข้อมูลต้นฉบับเอาไว้ได้

เราจะพบว่า จากทฤษฎีและงานวิจัยตามที่ได้กล่าวมา บล็อกเชนได้มีคุณสมบัติในการสร้างความเชื่อมั่น โปร่งใส พร้อมตรวจสอบระบุตัวตนได้เป็นอย่างดี บล็อกเชนจึงมีความเหมาะสมที่จะนำมาใช้เป็นเครื่องมือสนับสนุนการสับเปลี่ยนเอกสารธุรกรรมทางอิเล็กทรอนิกส์ระหว่างหน่วยงานภาครัฐ

3. วิธีดำเนินการวิจัย

การวิจัยครั้งนี้มุ่งพัฒนากรอบสถาปัตยกรรมการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ภาครัฐที่มีประสิทธิภาพและความมั่นคงปลอดภัยด้วยเทคโนโลยีบล็อกเชนเพื่อรองรับการมุ่งสู่การพัฒนาเศรษฐกิจดิจิทัลอย่างยั่งยืนของประเทศไทย เป็นการวิจัยแบบผสมผสาน ระหว่างเชิงคุณภาพและเชิงปริมาณ เริ่มจากการศึกษาข้อมูลพื้นฐานที่เป็นยุทธศาสตร์ นโยบาย หลักการ ทฤษฎีและงานวิจัยที่เกี่ยวข้อง แล้วนำไปสร้างเครื่องมือในการสัมภาษณ์เชิงลึกกับผู้เชี่ยวชาญ หลังจากนั้นจึงทำการสังเคราะห์ข้อมูลเพื่อออกแบบและพัฒนากรอบสถาปัตยกรรมการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ และนำไปทดลองใช้ในสำนักงานคณะกรรมการอาหารและยา (อย.)

ผู้วิจัยนำเครื่องมือที่เป็นแบบสอบถามกึ่งโครงสร้างไปสัมภาษณ์เชิงลึกกับผู้เชี่ยวชาญ ในที่นี้ ผู้วิจัยได้คัดเลือกผู้เชี่ยวชาญแบบเจาะจงเลือกที่เป็นผู้รู้ลึก และรู้จริง จำนวนน้อยไม่น้อยกว่า 8 คน [21] ในที่นี้ผู้วิจัยใช้จำนวนทั้งสิ้น 25 คน แบ่งออกเป็นผู้เชี่ยวชาญ 7 กลุ่ม คือ 1. ผู้เชี่ยวชาญด้านธุรกรรมอิเล็กทรอนิกส์ 2. ผู้เชี่ยวชาญด้านสถาปัตยกรรมองค์กร 3. ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ 4.ผู้เชี่ยวชาญด้านเทคโนโลยีบล็อกเชน 5. ผู้เชี่ยวชาญด้านเศรษฐกิจดิจิทัล 6. ผู้เชี่ยวชาญด้านเทคโนโลยีดิจิทัล และ 7. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง จากกระทรวงต่าง ๆ (ข้อที่ 1-6 จำนวนละ 3 คน ข้อที่ 7 จำนวน 7 คน)

จากนั้น ผู้วิจัยได้นำข้อมูลที่สัมภาษณ์เชิงลึกมาทำการวิเคราะห์เนื้อหา (Content Analysis) โดยวิเคราะห์และสังเคราะห์จากกลุ่มคำหลัก เพื่อให้ได้แนวทางในการพัฒนาสถาปัตยกรรมการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ที่มีประสิทธิภาพและความมั่นคงปลอดภัยด้วยบล็อกเชน ผู้วิจัยยังได้ออกแบบ

ตารางที่ 1 *ความสัมพันธ์ของกลุ่มคำและคำหลัก*

กลุ่มคำ	ความสัมพันธ์	คำหลัก
- ควรมีการตรวจสอบความถูกต้องได้โดยทุกคนหรือหน่วยงานที่เกี่ยวข้อง - รูปแบบวิธีการสับเปลี่ยนเอกสารในเครือข่ายควรที่จะรองรับความถูกต้องของรูปแบบเอกสารที่หลากหลายตามความต้องการของหน่วยงานที่จะสับเปลี่ยนเอกสารระหว่างกัน - แพลตฟอร์มการสับเปลี่ยนเอกสารการทำธุรกรรมอิเล็กทรอนิกส์ระหว่างหน่วยงานภาครัฐ จะต้องมีคุณสมบัติที่สามารถยืนยันได้ว่าเอกสารที่สับเปลี่ยนผ่านแพลตฟอร์มนี้ถึงผู้รับที่ถูกต้องตรงตามเจตนารมณ์ของผู้รับและผู้ส่งเอกสาร - ควรมีกลไกการตรวจสอบว่าข้อมูลต้นฉบับไม่ถูกเปลี่ยนแปลง (Tamper proof for immutable data) คำนึงถึงหลักพื้นฐานความถูกต้องครบถ้วน - ควรมีการตรวจสอบย้อนถึงแหล่งข้อมูลต้นทาง (Traceability) - ควรมีการตรวจความใช้ได้ (Validation) ต้องมีกลไกการตรวจสอบความถูกต้องของข้อมูลตั้งต้นว่าไม่มีการปลอมแปลง หรือนำเข้าข้อมูลที่ไม่ถูกต้องตามการกำหนดอายุการจัดเก็บ (Data Retention)	เป็นส่วนหนึ่งของกรอบสถาปัตยกรรม	เครือข่ายแห่งความถูกต้องครบถ้วน

กลุ่มคำ	ความสัมพันธ์	คำหลัก
- ควรยึดตามหลักพื้นฐานของบล็อกเชน ที่โครงสร้างจะไม่ได้อยู่ในความรับผิดชอบของหน่วยใดหน่วยหนึ่งแต่จะมีการเป็น Decentralized Concept ที่แต่ละหน่วยงานต่างนำทรัพยากรมาช่วยกันสร้างและช่วยกันใช้ - การดำเนินการจะต้องยึดหลัก Collaboration มากกว่าไปกำหนดว่าหน่วยงานใดต้องรับผิดชอบเพียงหน่วยงานเดียว	เป็นส่วนหนึ่งของกรอบสถาปัตยกรรม	ความสามารถของการทำงานเชิงกระจาย
- ด้านโครงสร้างพื้นฐานเพื่อการจัดเก็บข้อมูลควรมีความมั่นคงปลอดภัยในรูปแบบกระจายโดยใช้บล็อกเชนสมาร์ตคอนแท็ก ควรต้องคำนึงถึงขั้นตอนการออกแบบในเรื่อง Security in Design และ Privacy in Design การทดสอบ Penetration Test ควรนำมาใช้ตั้งแต่ขั้นตอนการ Implement จนกระทั่งเมื่อเปิดใช้งาน - ด้านความปลอดภัยควรมีการดำเนินการโดยอิงมาตรฐาน เช่น ISO 27000 Series - ควรคำนึงถึง Secure Authentication ของผู้ใช้งานโดยใช้ Digital ID - ควรคำนึงถึง การเข้ารหัสข้อมูล เพื่อความปลอดภัยแล้วยังจำเป็นต้องแนบใบลายเซนต์ดิจิตอลผ่านการทำ Certificate เพื่อความปลอดภัยและความเชื่อใจในเจ้าของข้อมูลและผู้รับข้อมูล - ควรคำนึงถึงการทำ Monitoring เพื่อตรวจวัดและประเมินความมั่นคงปลอดภัย และความพร้อมใช้ - มีการใช้เทคโนโลยีสนับสนุนการสื่อสารอย่างปลอดภัยระหว่างโหนดด้วย Transport Layer Security (TLS)	เป็นส่วนหนึ่งของกรอบสถาปัตยกรรม	ความมั่นคงปลอดภัย
-ควรใช้เทคโนโลยีบล็อกเชน ร่วมกับระบบที่สมาร์ตเพื่อช่วยทำการเชื่อมโยงหน่วยงานต่าง ๆ ที่เกี่ยวข้องเข้าด้วยกันผ่านทางออนไลน์แบบอัตโนมัติ	เป็นส่วนหนึ่งของกรอบสถาปัตยกรรม	การมีส่วนร่วม
- ด้านเทคโนโลยีบล็อกเชน ต้องโปร่งใส ตรวจสอบได้ - ควรคำนึงถึงหลักพื้นฐานความถูกต้วน มีกลไกการตรวจสอบว่าข้อมูลต้นฉบับไม่ถูกเปลี่ยนแปลง (Tamper Proof for Immutable Data) - ควรมีการจัด Data Classification ของข้อมูล โดยแยกหรือจำกัดข้อมูลส่วนบุคคลออกได้	เป็นส่วนหนึ่งของกรอบสถาปัตยกรรม	ความโปร่งใสสามารถตรวจสอบได้
- ควรคำนึงถึง Transparency เพื่อสร้างความเชื่อมั่นและความไว้วางใจ โดยใช้ บล็อกเชน - ควรมีการรักษาความเป็นส่วนตัว (Privacy) โดยอาจต้องอ้างอิงกับ GDPR	เป็นส่วนหนึ่งของกรอบสถาปัตยกรรม	ความไว้วางใจ
- ควรมีระบบโทเคนในการเข้าถึงข้อมูลด้วยสิทธิแบบต่าง ๆ ตามข้อกำหนดของผู้บริหารจัดการข้อมูล - ควรออกแบบและสร้างโพรโทคอลแลกเปลี่ยนเอกสารโดยวางกลไกของ Data Provider และ Data Consumer โพรโทคอล สามารถเปิดการเข้าถึงข้อมูลโดย Data Provider และให้ Data Consumer เข้าถึงด้วยสิทธิ์ที่กำหนด ผ่านกลไกของ Trusted Path - ระบบต้องสามารถรองรับกำหนดสิทธิ์ เข้าใช้งาน และการร้องขอต้องได้รับการยินยอมจากเจ้าของเอกสาร ซึ่งต้องมีการกำหนดนโยบายต่าง ๆ ไว้รองรับให้ใช้งานนั่นคือควรจะเป็น Private Permission Blockchain - เครือข่ายบล็อกเชน ควรเป็นระบบปิดให้เข้าร่วมเฉพาะผู้ที่ได้รับอนุญาตเท่านั้นหรือที่เรียกว่า Permission Blockchain ผ่าน Certificate Authority (CA)	เป็นส่วนหนึ่งของกรอบสถาปัตยกรรม	การเข้าถึงสิทธิ์
- ควรใช้เทคโนโลยีการประมวลผลแบบ Distributed Ledger ที่ทุกโหนดในบล็อกเชน ต้องแชร์ข้อมูลกัน โดยข้อมูลจะเห็นเฉพาะผู้ที่เข้าร่วมหรือได้รับอนุญาตเท่านั้น - ควรมีระบบควบคุมการเข้าถึงทรัพยากรของผู้เข้าร่วมแต่ละคน กำหนดสมาชิกและบทบาทของแต่ละสมาชิกที่อยู่ภายใต้เครือข่าย - ควรใช้หลักโปรโตคอล Consensus แบบโหนดเชื่อมถึงกันหมดและโหนดจะทำงานในระบบได้ จะต้องเป็นโหนดที่ถูกกำหนดโดยผู้ดูแลระบบเท่านั้น - ควรคำนึงถึงหลักพื้นฐานความลับมีการเข้ารหัสด้วยขั้นตอนวิธีที่แข็งแกร่ง น่าเชื่อถือและมีประสิทธิภาพ เช่น AES256-GCM		
- ควรมีหน่วยงานกำหนดมาตรฐานกลาง คล้าย ๆ NISt USA - ควรมีการสร้างหลักประกันเพื่อป้องกันการปฏิเสธความรับผิดชอบในการรับส่งเอกสารอิเล็กทรอนิกส์ผ่านแพลตฟอร์มการสับเปลี่ยนเอกสาร ฯ (Non Repudiation) เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์เป็นไปได้อย่างต่อเนื่องจนจบกระบวนงาน - ควรมี Availability เพื่อสร้างความมั่นใจให้ผู้ใช้บริการแพลตฟอร์มสับเปลี่ยนเอกสารฯได้ว่า เอกสารที่สับเปลี่ยนผ่านแพลตฟอร์มจะไม่มีบุคคลอื่นใดนอกจากผู้รับและผู้ส่งสามารถเข้าถึงเอกสารและเอกสารที่สับเปลี่ยนไม่ถูกแก้ไขเปลี่ยนแปลงหลังจากที่ถูกจัดทำขึ้นมา - ควรมีหน่วยงานกลางในการกำหนดกรอบนโยบายในการสับเปลี่ยนเอกสาร เพื่อให้มีความปลอดภัยสามารถกำหนดการเห็นธุรกรรมที่เกิดขึ้นเฉพาะภายในกลุ่มสมาชิกที่ถูกระบุเท่านั้น	เป็นส่วนหนึ่งของกรอบสถาปัตยกรรม	เครือข่ายแห่งความถูกต้องครบถ้วน

และนำไปทดลองเชิงปฏิบัติการใช้ในสำนักงานคณะกรรมการอาหารและยา (อย.) ณ สำนักงานจังหวัดนนทบุรี

4. ผลการวิจัย

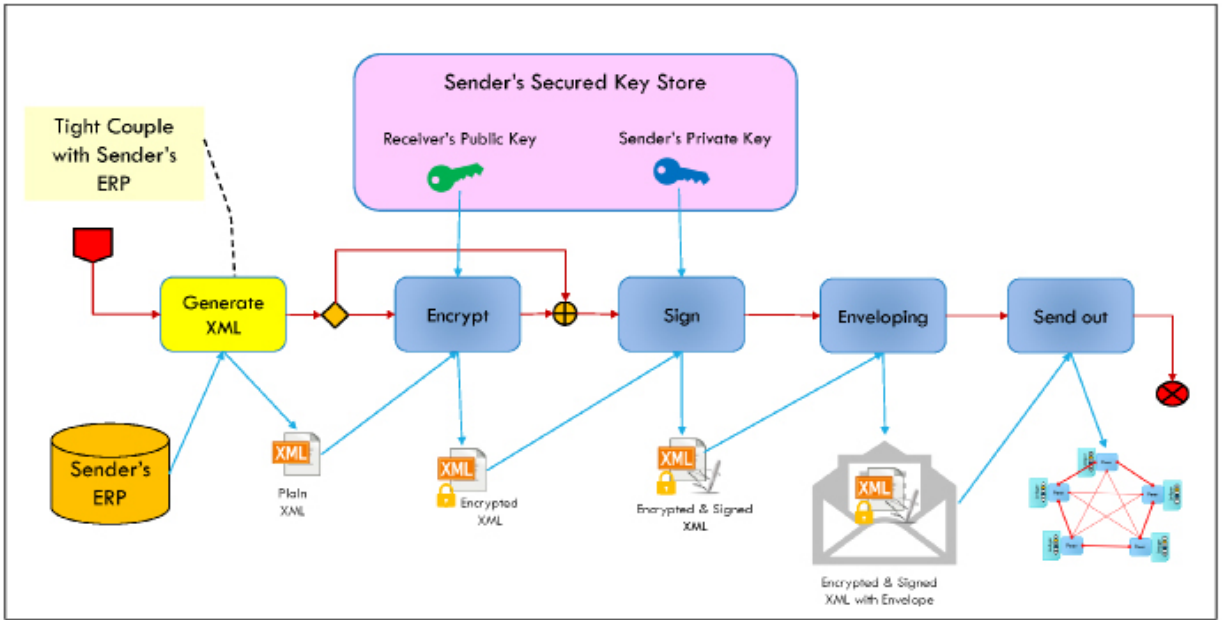
จากการวิจัยเชิงคุณภาพที่เป็นการศึกษาข้อมูลยุทธศาสตร์ นโยบายของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม หลักการ ทฤษฎีและงานวิจัยที่เกี่ยวข้อง รวมทั้งข้อมูลจากการสัมภาษณ์เชิงลึกกับผู้เชี่ยวชาญ พบว่า ผลสรุปวิเคราะห์เนื้อหาจากการสัมภาษณ์ที่ใช้คำหลักมาแยกเป็นกลุ่มคำสำคัญนั้น สามารถแบ่งออกได้ทั้งสิ้น 8 กลุ่มคำ มีดังนี้

ผลการวิเคราะห์ข้อมูลจากการสัมภาษณ์ผู้เชี่ยวชาญตามในตารางที่ 1 พบว่า มีประเด็นที่สำคัญอันนำไปสู่การออกแบบสถาปัตยกรรมการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ระหว่างหน่วยงานภาครัฐให้มีประสิทธิภาพและความมั่นคงปลอดภัยด้วยเทคโนโลยีบล็อกเชนนั้น ผู้วิจัยพบว่าการจัดการเอกสารภาครัฐ มีความจำเป็นอย่างยิ่งที่จะต้องมีการอำนวยการจัดการแก้ปัญหาความยุ่งยากในขั้นตอนที่มีจำนวนมาก ดังนั้นผู้วิจัยจึง

ได้ทำการออกแบบการรับ-ส่งข้อมูลที่มีชั้นความลับระหว่างหน่วยงานภาครัฐภายใต้สถาปัตยกรรมที่ได้พัฒนาขึ้น ได้แก่ ข้อมูลที่มีชั้นความลับต่าง ๆ ตามทางราชการกำหนดและหน่วยงานได้ส่งเอกสารมาเพื่อขอรับใบอนุญาต เป็นต้น

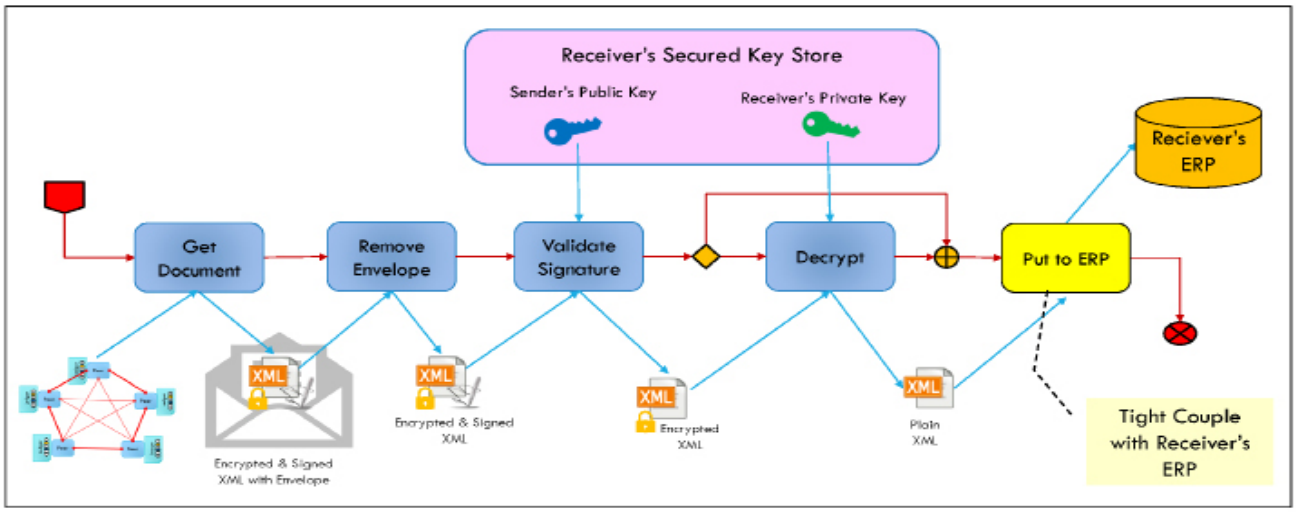
การออกแบบสถาปัตยกรรมการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ระหว่างหน่วยงานภาครัฐได้คำนึงถึงความถูกต้องของเครือข่าย การกระจายอำนาจ ความมั่นคงและความปลอดภัย การมีส่วนร่วม ความโปร่งใส สามารถตรวจสอบได้ ความไว้วางใจ การเข้าถึงสิทธิ์ และมาตราฐานสากล ผู้วิจัยได้เพิ่มเติมวิธีการที่นำ กุญแจ (Key) ไปใช้สำหรับการเข้ารหัสแบบสมมาตรของ ของดิฟฟีและเฮลแมน มาเข้ารหัสเอกสารที่ใช้รับ-ส่ง พร้อมทั้งการใช้ลายมือชื่ออิเล็กทรอนิกส์ ร่วมกับเทคโนโลยีบล็อกเชน โดยการกำหนดขั้นตอนการ ส่ง-รับ เอก สารประกอบด้วย การจัดเตรียมข้อมูลในเอกสารรูปแบบ XML การเข้ารหัส การลงลายมือชื่ออิเล็กทรอนิกส์การบรรจุเข้าซอง และการจัดเก็บในบล็อกเชน ซึ่งแนวคิดนี้ ดิฟฟี และเฮลแมน ได้พัฒนาอัลกอริทึมสับเปลี่ยนกุญแจ (Key Exchange Algorithm) เพื่อใช้รับ-ส่ง เอกสารผ่านเครือข่ายให้ข้อมูลมีความมั่นคงปลอดภัย

อย่างไรก็ดี เพื่อให้เป็นการเข้าใจในกระบวนการบรรจุซองจดหมาย เอกสารที่จะส่ง จะถูกเข้ารหัสทั้งไฟล์ในรูป Base 64 และบันทึกลงในแท็กเนื้อหา (Content Tag) ของซองจดหมาย โดยวิธีนี้โครงสร้างของเอกสารประกอบการขออนุญาตจะเป็นความรับผิดชอบระหว่างผู้รับและผู้ส่ง ในขณะที่โครงสร้างของซองจดหมายจะเป็นความรับผิดชอบระหว่างผู้รับกับผู้ส่ง และผู้ให้บริการแพลตฟอร์ม โดยที่ผู้ให้บริการแพลตฟอร์มไม่มีความจำเป็นต้องเข้าใจโครงสร้าง (Schema) ของเอกสารประกอบการขออนุญาตที่รับ-ส่ง แต่อย่างใด ซองจดหมายจะเข้ารหัสหรือลงนามโดยใช้กุญแจส่วนตัว (Private Key) ของเครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่เชื่อมต่อ (Gateway) กับแพลตฟอร์มเพื่อยืนยันสิทธิในการใช้บริการ (Authentication) ก่อนจะส่งเข้าแพลตฟอร์มต่อไปดังแสดงในภาพที่ 2

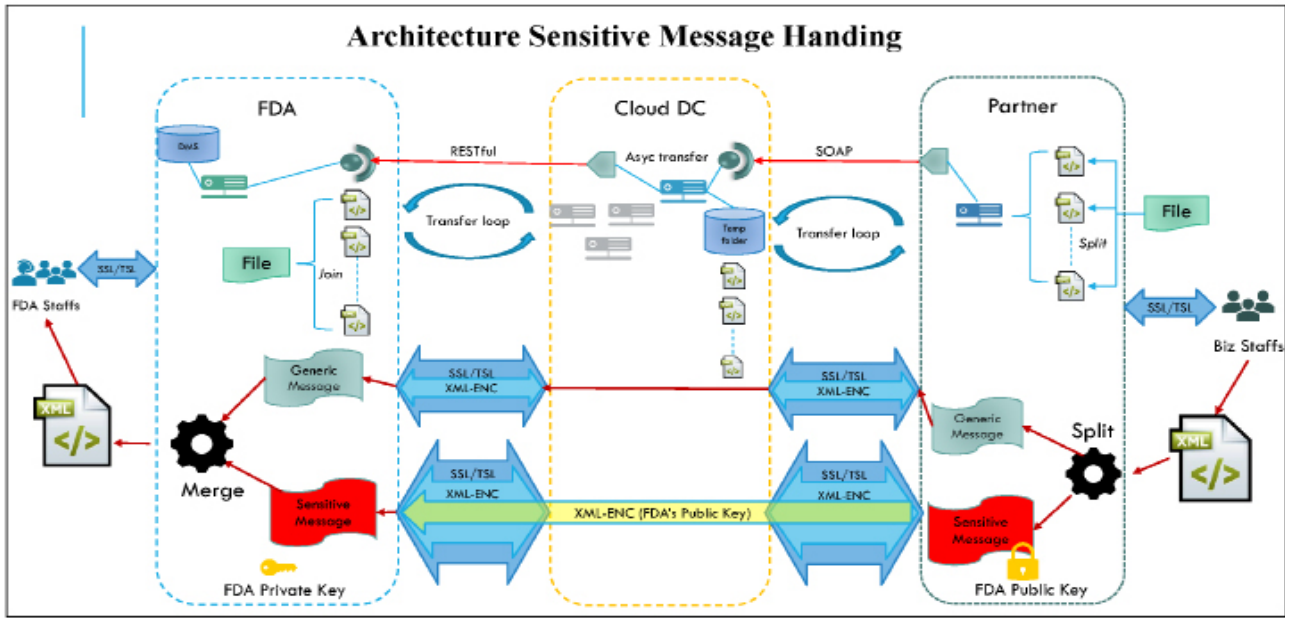


ภาพที่ 2 *ขั้นตอนการส่งเอกสารผ่านเครือข่ายบล็อกเชน*

การรับเอกสารจะเป็นกระบวนการย้อนกลับของการส่งเอกสารกล่าวคือ ผู้รับจะตรวจสอบความถูกต้องในการส่งเอกสารโดยตรวจสอบชื่อผู้รับปลายทางจากแท็กผู้รับ (Receiver Tag) ของซองจดหมายเพื่อให้แน่ใจว่าเอกสารนั้นจัดส่งให้ตนอย่างถูกต้อง จากนั้นจะคัดแยก (Extract) เอกสารที่ส่งจากแท็กเนื้อหา (Content Tag) ของซองจดหมายแล้วถอดรหัส จากรูปแบบ Base 64 กลับเป็น ไฟล์ XML ตามปกติเอกสารประกอบการขออนุญาตที่ถูกคัดแยกออกจากซองจดหมายแล้วจะได้รับการตรวจสอบและถอดรหัสโดยใช้กุญแจสาธารณะ (Public Key) ของผู้ส่งและกุญแจส่วนตัวของผู้รับ ดังแสดงในภาพที่ 3



ภาพที่ 3 แสดงขั้นตอนการรับเอกสารผ่านเครือข่ายบล็กเชน



ภาพที่ 4 แสดงขั้นตอนการรับ - ส่งเอกสารที่มีชั้นความลับ

ผู้วิจัยได้มีการนำกรอบสถาปัตยกรรมการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ระหว่างหน่วยงานภาครัฐตามภาพที่ 2 และภาพที่ 3 ไปทดลองใช้ในสำนักงานคณะกรรมการอาหารและยา (อย.) บล็อกเชนที่จะใช้งานจะได้รับการออกแบบโดยคำนึงถึงความเป็นส่วนตัวของข้อมูล (Data Privacy) ในเอกสารที่รับส่งระหว่างกัน ดังที่สรุปได้จากบทสัมภาษณ์ แม้งานขออนุญาตผลิตภัณฑ์สุขภาพของสำนักงานคณะกรรมการอาหารและยาจะเป็นงานบริการสาธารณะ แต่ข้อมูลต่าง ๆ ที่ใช้ในการประกอบการขออนุญาตจัดเป็นความลับทางการค้า จึงไม่อาจเปิดเผยต่อสาธารณะได้ ยกเว้นแต่จะมีคำสั่งศาลหรือคำสั่งทางปกครองให้เปิดเผยแล้วเท่านั้น การใช้บล็อกเชนเพื่อรับส่งเอกสารการขออนุญาตจึงต้องอาศัยเทคโนโลยีการเข้ารหัส (Encryption Technology) ในการเข้ารหัสเอกสารเพื่อให้ผู้รับเอกสารที่ได้รับอนุญาตให้เข้าถึงข้อมูลในเอกสารเท่านั้น ที่จะสามารถอ่านเอกสารได้ ในกรณีศึกษานี้กำหนดให้ใช้เทคโนโลยีกุญแจคู่ (PKI) ในการเข้ารหัสเอกสาร หลังจากที่จัดทำเอกสารที่พร้อมจะส่งให้ผู้รับขึ้นมาแล้ว ระบบสารสนเทศของผู้ส่งเอกสารจะเข้ารหัสเอกสารโดยใช้กุญแจสาธารณะของผู้รับและกุญแจส่วนตัวของผู้ส่ง ทำให้ผู้ที่ถือครองเอกสารนั้น ต้องอาศัยกุญแจสาธารณะของผู้ส่ง และกุญแจส่วนตัวของผู้รับในการถอดรหัสเอกสารเพื่อเปิดอ่าน ผู้ถือครองเอกสารที่ไม่มีกุญแจทั้งสองชุดจะไม่สามารถเปิดเอกสารอ่านได้ ด้วยเหตุที่แพลตฟอร์มบล็อกเชนนี้ ได้รับการออกแบบให้รองรับการรับและส่ง เอกสารระหว่างหลายหน่วยงาน มีความแม่นยำในการส่งเอกสารให้ผู้รับที่ถูกต้องตรงกับเจตนาของผู้ส่ง ในประเด็นนี้จึงเป็นสิ่งสำคัญอย่างยิ่งยวดสำหรับเอกสารภาครัฐ

ดังนั้น เพื่อเพิ่มความถูกต้องแม่นยำในการส่งเอกสารให้ผู้รับที่ถูกต้อง เอกสารที่จะส่ง จะถูกบรรจุลงในไฟล์รูปแบบ XML ซึ่งมีโครงสร้าง (Schema) ที่เรียบง่ายทำหน้าที่เป็นซองจดหมาย โดยมีแท็กที่ระบุตัวผู้รับและผู้ส่งรวมทั้งประเภทเอกสารไว้อย่างชัดเจน (Mandatory Tag) หลังจากที่แพลตฟอร์มได้รับเอกสารแล้วจะตรวจสอบชื่อผู้รับปลายทางจากแท็กผู้รับ (Receiver Tag) แล้วส่งเอกสารต่อไปให้ผู้รับพร้อมกับจัดเก็บเอกสารเข้าบล็อกเชน อย่างไรก็ตาม มีเอกสารบางประเภทที่จะไม่ได้รับการจัดเก็บเข้าบล็อกเชน เอกสารประเภทนี้ได้แก่ ข้อมูลคุณลักษณะเฉพาะของผลิตภัณฑ์ อาทิ สูตรส่วนประกอบ ข้อมูลการวิจัยผลิตภัณฑ์หรือข้อมูลอื่นใดที่จะก่อให้เกิดความเสียหายทางการค้าต่อผู้ส่งเอกสาร เป็นต้น หากถูกเปิดเผยโดยไม่ได้รับอนุญาตจากผู้ส่งเอกสาร กุญแจสาธารณะของผู้ส่งไม่สามารถใช้ถอดรหัสได้ จะหมายความว่า กุญแจของผู้ส่งไม่ถูกต้องหรือผู้ส่งระบุผู้รับผิดพลาด และผู้ถือครองเอกสารจะไม่สามารถอ่านเอกสารที่ได้รับดังแสดงในภาพที่ 4

จากการที่ผู้วิจัยนำไปทดลองใช้ในสำนักงานคณะกรรมการอาหารและยา (อย.) ยังพบอีกว่าบล็อกเชนที่ออกแบบมานั้นสามารถลำดับชั้นความลับตามแบบเอกสารราชการและมีการยืนยันความถูกต้องในการรับและส่งเอกสารและตลอดจนสามารถนำไปใช้อ้างอิงในกระบวนการยุติธรรมได้ แก้ปัญหาจัดการรับและส่งเอกสารภาครัฐ ภาคเอกชน และภาคประชาชน ได้อย่างมีประสิทธิภาพ

5. สรุป

ปัญหาของการติดต่อสื่อสารแลกเปลี่ยนข้อมูลในหน่วยงานภาครัฐหรือหน่วยงานใด ๆ กับภาคราชการ คือ ความซับซ้อนและมากขั้นตอน กรอบสถาปัตยกรรมการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ที่ผู้วิจัยได้พัฒนาขึ้นนี้สามารถลดปัญหา เพิ่มประสิทธิภาพในการประสานงานในหน่วยงานของภาครัฐด้วยกัน หรือหน่วยงานเอกชนประสานงานติดต่อกับภาครัฐ ตลอดจนประชาชนติดต่อกับภาครัฐได้เป็นอย่างดี ในงานวิจัยนี้ได้เพิ่มการรับ-ส่ง เอกสารร่วมกับเทคโนโลยีการเข้ารหัสแบบสมมาตรของดิฟฟี-เฮลแมน เพื่อเข้ารหัสเอกสารที่ใช้รับ-ส่ง พร้อมด้วยการใช้ลายมือชื่ออิเล็กทรอนิกส์ และเทคโนโลยีบล็อกเชน สำหรับกำหนดขั้นตอนการส่ง-รับ เอกสาร ซึ่งสามารถแก้ปัญหาลดความซับซ้อนและลดขั้นตอนการสับเปลี่ยนเอกสารภาครัฐได้อย่างมีประสิทธิภาพ ผู้วิจัยได้นำกรอบสถาปัตยกรรมการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ไปทดลองใช้ในสำนักงานคณะกรรมการอาหารและยา (อย.) พบว่าบล็อกเชนที่ออกแบบมานั้นใช้งานง่ายและมีความมั่นคงปลอดภัย ช่วยอำนวยความสะดวก เพิ่มความรวดเร็ว ลดขั้นตอนการติดต่อกับเจ้าหน้าที่ภาครัฐ ติดตามงาน

ได้ในทุกขั้นตอน สร้างความโปร่งใสในการทำงานของการให้บริการภาครัฐได้อย่างแท้จริง

6. เอกสารอ้างอิงข้อมูล

[1] R.C. Merkle, "A Digital Signature Based on a Conventional Encryption Function." *Advances in Cryptology — CRYPTO '87*. pp. 369-378., 1987.

[2] S. Haber, and W.S. Stornetta, "How to time-stamp a digital document." *Journal of Cryptology*. Vol.3, pp. 99–111, 1991.

[3] S. Nakamoto, *Bitcoin: A peer to peer electronic cash system.* Available Online at http://www.bitcoin.org/bitcoin.pdf, accessed on 15 January 2020.

[4] D. Tapscott, and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*. Penguin Pub., 2018.

[5] Office of the National Economics and Social Development Council. *20 Years National Strategy (2018-2037)*, 2019.

[6] Ministry of Information and Communication Technology. *Information and Communication Technology Policy Framework for the period (2011-2020)*, 2011.

[7] Ministry of Digital Economy and Society. *Thailand Digital Economy and Society Development Plan (2018-2037)*, 2010.

[8] Office of the National Economics and Social Development Council. *National Economic and Social Development Plan.Issue no. 12 (2017-2021)*, 2019.

[9] Office of the National Economics and Social Development Council. *Strategic Plan for Logistics Development in Thailand.Issue no.3(2017-2021)*, 2017.

[10] ISO/IEC20000- 1:2018. *Information technology-Service management*. Switzerland, 2018.

[11] ISO/IEC 27001:2018: *Information Technology – Security Techniques – Information Security Management Systems - Requirements.* Switzerland, 2018.

[12] National Institute of Standard and Technology (NISt). *NISt 800-53 rev 4 - Security and Privacy Controls for Federal Information Systems and Organizations.* 2013.

[13] ISO/IEC 27005:2018: *Information technology - Security techniques - Information security risk management*. Switzerland, 2018.

[14] W. Diffie, and M.E. Hellman, "New Directions in Cryptography." *IEEE Transactions on Information Theory.* Vol. IT-22 (6): pp.644–654, November, 1976.

[15] M.H.M. Schellekens, *Electronic Signatures: Authentication Technology from a Legal Perspective*, T.M.C. Asser Press, 2004.

[16] T. Santhanamery, and T. Ramayah, "Continued Usage Intention of E-Filing: The Role of Optimism Bias." *Procedia - Social and Behavioral Sciences*. Vol. 65.No.1. pp. 397 – 403, 2012.

[17] P. Ractham, P. "The Factors and Strategy toPersuade the Use of NSW." *NIDA Business Journal.* No.16. pp.26-59, 2015.

[18] Tierion. *Blokhain Healthcare 2016 Report – Promise & Pitfalls.* Available Online at https://tierion.Com/blog/Blockchain-healthcare-2016-report/, accessed on 15 January 2020.

[19] W.K. Meijer, D. Middendorp, J.M. Raes, and R. Tubbing, "Digital Voting Pass." *Thesis of the Delft University of Technology.* Netherlands, 2017.

[20] D.A. Wijaya, J.K. Liu, D.A. Suwarsono, and P. Zhang, "A New Blockchain-Based Value-Added Tax System." *in Proceeding of 11th International Conference, ProvSec 2017*, China, 2017.

[21] Kijpredaborisuthi, B., (2010). *Data Collection Tools for Research*. 7th Edition. Bangkok: Si Anan Printing Co.,Ltd, 2010.