การพัฒนาตัวแบบจำลองด้วยบล็อกเชนสำหรับการจัดเก็บข้อมูลประวัติอาชญากรรมและบูรณาการกระบวนการยุติธรรมในประเทศไทย

A Development of Blockchain based Model of Criminal Records and Justice Process Integrations in Thailand

*ชัยพร ทบแป**

Chaiporn Thoppae

*สมนึก คีรีโต, สุรศักดิ์ สงวนพงษ์, ศรายุทธ ฉายสุริยะ***

Somnuk Keretho, Surasak Sanguanpong, Sarayut Chaisuriya

*นวลศรี เด่นวัฒนา, อภิสิทธิ์ แสงใส, ณัฐพร ภักดี และมาโนชญ์ ใจกว้าง****

Nuansri Denwattana, Apisit Seangsai, Nuttaporn Phakdee, Manot Jaikwang

บทคัดย่อ

บล็อกเชนเป็นเทคโนโลยีที่มีศักยภาพในการเชื่อมโยงข้อมูลทำให้เกิดบูรณาการการปฏิบัติงานระหว่างหน่วยงานในกระบวนการยุติธรรมให้มีความโปร่งใส มีกลไกการตรวจสอบเพื่อป้องกันการดัดแปลงข้อมูล อันเป็นหลักฐานสำคัญที่จัดเก็บในระบบและช่วยทำให้การปฏิบัติงานด้านยุติธรรมมีความเป็นธรรมและมีประสิทธิภาพ ทั้งนี้ ด้วยการใช้เทคนิคการเข้ารหัสลับและการบันทึกข้อมูลแบบกระจายซึ่งไม่อาจเปลี่ยนแปลงได้อันเป็นคุณสมบัติประการสำคัญของบล็อกเชน งานวิจัยนี้เสนอให้เลือกใช้บล็อกเชนสำหรับองค์กรความร่วมมือ โดยเสนอให้หน่วยงานในกระบวนการยุติธรรมพัฒนาโหนดของเครือข่ายบล็อกเชน 3 หน่วยงานแรก คือ สำนักงานตำรวจแห่งชาติ

* *ผู้ช่วยจัดการฝ่ายแลกเปลี่ยนข้อมูล บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)*
Assistant Vice President Data Interchange Business Department, National Telecom Public Company Limited

** *ภาควิชาวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์*
Department of Computer Engineering, Kasetsart University

*** *คณะวิทยาการสารสนเทศ มหาวิทยาลัยบูรพา*
Faculty of Informatics, Burapha University

Received: *March 25, 2021* ***Revised:*** *September 20, 2021* ***Accepted:*** *September 20, 2021*

สำนักงานอัยการสูงสุด และสำนักศาลยุติธรรม โดยการเชื่อมโยงระบบสารสนเทศตามพันธกิจหลักภายในที่มีอยู่แล้วของหน่วยงานเหล่านั้นให้เป็นโหนดของบล็อกเชน จากนั้นให้มีหน่วยงานในกระบวนการยุติธรรม เช่น กรมราชทัณฑ์ และกรมคุมประพฤติ เป็นลำดับต่อไปที่สามารถเชื่อมโยงเป็นโหนดของบล็อกเชนด้วย

งานวิจัยนี้นำเสนอสถาปัตยกรรม และการออกแบบระบบเพื่อสร้างความมั่นคงปลอดภัยแบบวงแหวนหลายชั้น พร้อมข้อเสนอที่เป็นปัจจัยสำคัญสำหรับการพัฒนาบล็อกเชนให้เกิดสัมฤทธิ์ผล ซึ่งประกอบด้วยกลไกการเพิ่มประสิทธิภาพการประมวลผลของบล็อกเชน และการจัดการกับไฟล์ข้อมูลขนาดใหญ่ที่เป็นหลักฐานพยาน และประวัติอาชญากรรมด้วยระบบบริหารจัดการเอกสารควบคู่กับการใช้ค่าแฮช เพื่อพิสูจน์ความถูกต้องครบถ้วนของข้อมูล ตลอดจนการกล่าวถึงความสำคัญของการจัดเตรียมโหนดบล็อกเชนเพื่ออำนวยความสะดวกการประสานงาน และความสำคัญของบุคลากรด้านเทคนิคบล็อกเชน

คำสำคัญ: เทคโนโลยีบล็อกเชน, บล็อกเชนสำหรับองค์กรความร่วมมือ, การจัดเก็บข้อมูลประวัติอาชญากรรม, การเชื่อมโยงกระบวนการยุติธรรม

Abstract

Blockchain technology has the potential to increase transparency and efficiency by data connection and integrating operations between agencies in the justice process. Relying upon cryptography and immutable distributed data stores, the blockchain provides prevention mechanisms to data evidences from unauthorized alteration after the data were collected in the system, thereby, promoting efficiency and accountability in the inter-agency justice procedures. This research proposes the adoption of blockchain platform for private/consortium organizations. Initially, the first three government agencies that should establish their blockchain peer nodes are the Royal Thai Police, the Office of the Attorney General, and the Office of the Court of Justice. The capturing of upstream evidence and criminal data of the whole justice process under these three agencies should be integrated. The subsequent agencies that should also establish their blockchain peer nodes upon their readiness in human resources and internal information systems are the Department of Corrections and the Department of Probation.

This research presents a design of the system based on multi-layers secure architecture. Several critical success factors have been discussed especially those related to development and deployment, as well as mechanisms to increase the performance of blockchain transaction processing. The document management systems are also proposed for handling large data files along with the use of hashing functions to preserve the data integrity. The importance

of establishing the peer facilitator and preparing the blockchain technical personnel are also addressed.

Keyword: Blockchain Technology, Private/ Consortium Blockchain, Criminal Records Management, Justice Process Integration

บทนำ

เทคโนโลยีบล็อกเชนเป็นเทคโนโลยีที่มีกลไกช่วยเพิ่มความเชื่อมั่นของข้อมูลที่ถูกจัดเก็บในระบบว่าจะไม่ถูกแก้ไขโดยมิชอบได้ง่าย โดยใช้บล็อกเชนประกอบกับการเข้ารหัสข้อมูล (cryptography) และกระจายการจัดเก็บข้อมูลชุดเดียวกันแต่เก็บไว้ในที่จัดเก็บหลายแห่ง (distributed ledgers) นอกจากนี้ บล็อกเชนยังช่วยให้เกิดการประมวลผลธุรกรรมได้โดยไม่ต้องผ่านบุคคลที่สาม หรือไม่ต้องผ่านคนกลาง แต่ใช้การบันทึกข้อมูลธุรกรรมรวมกันเป็นกลุ่มข้อมูล (blocks) และให้ผู้มีอำนาจที่เกี่ยวข้องรับรองความถูกต้องของข้อมูลก่อนที่จัดเก็บในลักษณะห่วงโซ่ของกลุ่มข้อมูล (chain of blocks) บล็อกเชนจึงได้รับการยอมรับว่าเป็นเทคโนโลยีที่มีความปลอดภัยสูง ช่วยป้องกันการรั่วไหลของข้อมูล และสามารถเลือกเปิดเผยเฉพาะข้อมูลที่เกี่ยวข้องแก่บุคคลที่ได้รับการกำหนดสิทธิ์ได้ (Thoppae, Praneetpolgrang, & Jirawichitchai, 2021) ด้วยเหตุผลพื้นฐานดังกล่าว ภาครัฐของหลายประเทศ จึงให้ความสนใจและการศึกษาปัจจัยที่ส่งผลต่อความเป็นไปได้ที่จะนำเทคโนโลยีบล็อกเชนมาใช้ในการบริหารจัดการข้อมูล (ชัยพร ทบแป, ประสงค์ ประณีตพลกรัง และนิเวศ จิระวิชิตชัย, 2563) โดยเฉพาะอย่างยิ่งในการเก็บหลักฐานสำคัญหรือเอกสารแสดงสิทธิ์ต่าง ๆ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษา วิเคราะห์ประโยชน์ และความเป็นไปได้ของการนำบล็อกเชนมาใช้ในการจัดเก็บข้อมูลประวัติอาชญากรรม โดยเน้นผลกระทบด้านความมั่นคงปลอดภัยและความน่าเชื่อถือของข้อมูล โดยการออกแบบและพัฒนาแบบจำลอง (model) (Department of Defense Standard, 1985) รวมทั้งเสนอแนวทางการใช้บล็อกเชน เพื่อจัดเก็บข้อมูลของผู้กระทำความผิดพร้อมทั้งเชื่อมโยงกระบวนการยุติธรรมทางอาญาในประเทศไทย

เนื้อหาของบทความนี้แบ่งเป็น 8 ส่วน ได้แก่ ส่วนที่ 1 เป็นบทนำและคำอธิบายวัตถุประสงค์ของงานวิจัย ส่วนที่ 2 แสดงระเบียบวิธีวิจัยในโครงการนี้ส่วนที่3นำเสนอปัญหา และอุปสรรคในกระบวนการยุติธรรมของประเทศไทย ส่วนที่ 4 กล่าวถึงระบบสารสนเทศที่ถูกนำมาใช้ในกระบวนการยุติธรรมโดยหน่วยงานของรัฐที่เกี่ยวข้อง ส่วนที่ 5 นำเสนอเทคโนโลยีและตัวอย่างการประยุกต์ใช้บล็อกเชนสำหรับกระบวนยุติธรรมในต่างประเทศ ส่วนที่ 6 นำเสนอผลการออกแบบสถาปัตยกรรมและเทคนิคการพัฒนาระบบบล็อกเชนเครือข่ายกระบวนการยุติธรรมสำหรับประเทศไทย ส่วนที่ 7 อธิบายผลการประชาวิพากษ์จากการระดมความเห็นจากผู้เชี่ยวชาญบล็อกเชนและตัวแทนจากหน่วยงานในกระบวนการยุติธรรม และส่วนที่8 นำเสนอบทสรุปและข้อเสนอแนะ

ระเบียบวิธีวิจัย

งานวิจัยนี้มุ่งเน้นศึกษาปัญหาอุปสรรคในกระบวนการยุติธรรมทางอาญา ความเป็นไปได้และแนวทางในการนำบล็อกเชนมาใช้เพื่อประโยชน์ในการพัฒนาระบบสารสนเทศเพื่อจัดเก็บข้อมูลหลักฐานและข้อมูลประวัติอาชญากรรม (criminal records) และเชื่อมโยงกระบวนการยุติธรรมของหน่วยงานที่เกี่ยวข้องในประเทศไทย (ประดิษฐ์ แป้นทอง, 2558) ผู้วิจัยได้ทำการเก็บรวบรวมข้อมูลตั้งแต่เดือนมิถุนายน พ.ศ. 2563 – ตุลาคม 2563

เนื้อหางานวิจัยเป็นการสำรวจความคิดเห็นของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องในภาคส่วนต่าง ๆ ที่เกี่ยวข้อง และสำรวจระบบสารสนเทศในปัจจุบันของหน่วยงานรัฐด้านการดำเนินการยุติธรรมของประเทศและต่างประเทศ พร้อมทั้งนำเสนอผลการออกแบบสถาปัตยกรรมระบบเทคนิคในการออกแบบในส่วนสำคัญที่เกี่ยวข้องกับความมั่นคงปลอดภัย (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2560) การเพิ่มประสิทธิภาพของระบบ และการนำเสนอประเด็นที่เป็นปัจจัยความสำเร็จของระบบอีกด้วย

การศึกษาวิจัยเชิงคุณภาพ

งานวิจัยนี้เป็นการวิจัยแบบผสมผสาน (mixed method) ของ Creswell and Plano (2018) กล่าวคือ เป็นการวิจัยเชิงคุณภาพ (qualitative research) และการวิจัยเชิงปริมาณ (quantitative research) ประกอบด้วยการทบทวนวรรณกรรม ศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง พร้อมทั้งการออกแบบระบบกับผู้เชี่ยวชาญด้านเทคโนโลยีบล็อกเชนและการวิพากษ์โดยตัวแทนจากหน่วยที่เกี่ยวข้องในกระบวนการยุติธรรม นักวิชาการ และผู้เชี่ยวชาญด้านบล็อกเชน กำหนดกลุ่มผู้ให้ข้อมูลสำคัญเพื่อการศึกษาวิจัยเชิงคุณภาพโดยใช้วิธีการสัมภาษณ์เชิงลึก (in depth interview) กับกลุ่มตัวอย่างที่เป็นตัวแทนหน่วยงานในกระบวนการยุติธรรมที่เกี่ยวข้องกับการจัดเก็บ และใช้ประโยชน์จากข้อมูลประวัติอาชญากรรม หน่วยงานที่เกี่ยวข้องกับการจัดทำระบบบูรณาการ เชื่อมโยงและใช้ประโยชน์จากข้อมูลประวัติอาชญากรรม รวมทั้งผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและบล็อกเชน

ผู้ให้ข้อมูลสำคัญ (key informant) ในการวิจัยครั้งนี้โดยการสัมภาษณ์ และขอความคิดเห็นจากทั้งนักการเมือง ผู้บริหารและผู้ปฏิบัติงานในหน่วยงานราชการ ผู้บริหารในหน่วยงานเอกสารและองค์กรอิสระ ผู้เชี่ยวชาญด้านเทคโนโลยีบล็อกเชนนักกฎหมายและประชาชนในระดับต่าง ๆ ผู้ถูกสัมภาษณ์มาจากหน่วยงานหรือองค์กรต่าง ๆ อย่างน้อย 14 องค์กร/กลุ่ม ได้แก่ (1) สำนักงานรัฐมนตรี กระทรวงยุติธรรม (2) สำนักงานปลัดกระทรวงยุติธรรม (3) สำนักงานกิจการยุติธรรม กระทรวงยุติธรรม ซึ่งมีบทบาทหลักในการร่าง พ.ร.บ. ทะเบียนประวัติอาชญากรรมฯ และการประสาน/ดำเนินการศูนย์แลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม (Data Exchange Center: DXC) (4) ศูนย์ ICT สำนักงานตำรวจแห่งชาติ (5) สถานีตำรวจนครบาล ได้แก่ สน.ทองหล่อ (6) สถานีตำรวจภูธร ได้แก่ สถานีตำรวจภูธรแสนสุข จ.ชลบุรี และสถานีตำรวจภูธร จ.ราชบุรี (7) สำนักงานอัยการ (8) ศาลยุติธรรม (9) กรมพินิจและคุ้มครองเด็กและเยาวชน (10) กรมคุมประพฤติ (11) กรมราชทัณฑ์ (12) บริษัท/องค์กรธุรกิจ/ภาคประชาชน (13) องค์กร

อิสระด้านการช่วยเหลือผู้ต้องขัง อบรมชีวิต และพัฒนาการศึกษาของผู้พ้นโทษ อาทิ มูลนิธิบ้านพระพร และ (14) ผู้เชี่ยวชาญด้านเทคโนโลยีบล็อกเชนและนักกฎหมาย จำนวน 30 คน โดยวิธีการเลือกตัวอย่างแบบมีจุดมุ่งหมายของการศึกษาเป็นหลัก (purposeful selection) เพื่อให้ได้กลุ่มตัวอย่างที่มีคุณสมบัติภายใต้กรอบของการศึกษาวิจัยโดยต้องเป็นบุคคลที่อยู่ในตำแหน่งระดับการเมือง การบริหาร ผู้ปฏิบัติงานประชาชน และผู้เชี่ยวชาญเฉพาะทั้งด้านกระบวนการยุติธรรม กฎหมาย และเทคโนโลยีบล็อกเชน

การศึกษาวิจัยเชิงปริมาณ

การสำรวจความคิดเห็นใช้แบบสอบถามจากกลุ่มประชาชนผู้มีส่วนได้ส่วนเสียกับการจัดเก็บข้อมูลทะเบียนประวัติอาชญากรรม ซึ่งครอบคลุมถึงกลุ่มต่าง ๆ เช่น กลุ่มประชาชนผู้รับบริการจากสถานีตำรวจนครบาล และสถานีตำรวจภูธร ผู้เสียหาย จำเลย ผู้ถูกกล่าวหา ผู้อยู่ระหว่างกระบวนการพัฒนาพฤตินิสัย และผู้พ้นโทษจากระบบพัฒนาพฤตินิสัย กลุ่มประชากรที่ดำเนินการสำรวจความเห็นเชิงปริมาณ ได้แก่

1) กลุ่มประชาชนผู้รับบริการจากสถานีตำรวจในเขตกรุงเทพมหานคร (นครบาล) จำนวน 87 แห่ง

2) กลุ่มประชาชนผู้รับบริการจากสถานีตำรวจในพื้นที่จังหวัดอื่น (ภูธร) โดยสุ่มเลือกจากจังหวัดที่มีปัญหาการเกิดอาชญากรรมมากเป็นพิเศษ ได้แก่ จังหวัดชลบุรี จังหวัดนครศรีธรรมราช จังหวัดเชียงใหม่ และจังหวัดนครราชสีมา (สำนักงานสถิติแห่งชาติ, 2563)

3) กลุ่มผู้เกี่ยวข้องกับคดีอาชญากรรมในลักษณะต่าง ๆ เช่น ผู้เสียหาย จำเลย ผู้ถูกกล่าวหา

4) กลุ่มผู้อยู่ระหว่างกระบวนการพัฒนาพฤตินิสัยในลักษณะต่าง ๆ เช่น ผู้ต้องขัง ผู้ถูกคุมประพฤติ และเด็กและเยาวชนในความดูแลของกรมพินิจและคุ้มครองเด็กและเยาวชน

5) กลุ่มผู้พ้นโทษจากระบบพัฒนาพฤตินิสัยในลักษณะต่าง ๆ

การกำหนดขนาดตัวอย่างและเลือกตัวอย่าง

การวิจัยเชิงคุณภาพ ใช้วิธีการเลือกตัวอย่างแบบเจาะจง (purposive sampling) โดยลักษณะของกลุ่มที่เลือกเป็นไปตามวัตถุประสงค์ของการวิจัย เนื่องจากต้องอาศัยความรอบรู้ความชำนาญและประสบการณ์ในเรื่องนั้น ๆ

การวิจัยเชิงปริมาณ โดยพิจารณาวัตถุประสงค์ของการศึกษาครั้งนี้ ซึ่งพบว่า ขนาดตัวอย่างที่เหมาะสมกับโครงการสำรวจครั้งนี้จะเป็นการกำหนดขนาดตัวอย่างที่สอดคล้องกับการเลือกตัวอย่างโดยคำนึงถึงค่าผลกระทบจากการเลือกตัวอย่างที่มากกว่า 1 ชั้น ด้วยความเชื่อมั่นร้อยละ 95 และความคลาดเคลื่อนบวกลบร้อยละ 5 ใช้การสุ่มตัวอย่างเชิงชั้นภูมิหลายชั้น (stratified multi-stage sampling) จากนั้นใช้การเลือกตัวอย่างแบบเชิงระบบ (systematic sampling) ในการเลือกตัวอย่าง และทำการเลือกตัวอย่างแบบง่าย (simple random sampling) เพื่อให้ได้ตัวอย่างครบตามจำนวนที่ต้องการตามสัดส่วนของประชากร และได้จำนวนกลุ่มตัวอย่างที่ดีที่สุด จำนวน 1,643 ตัวอย่าง (Comrey & Lee, 2013)

การออกแบบระบบ และพัฒนาแบบจำลอง

งานในส่วนนี้ประกอบด้วยการวิเคราะห์ปัญหาอุปสรรคในกระบวนการยุติธรรมส่วนที่เกี่ยวข้องกับการจัดเก็บหลักฐานทางกฎหมายและประวัติอาชญากรรมในประเทศไทย และพิจารณาความเป็นไปได้ในการประยุกต์บล็อกเชนเพื่อลดหรือแก้ไขปัญหาดังกล่าว

แล้วนำมาจัดทำข้อเสนอและออกแบบแบบจำลอง (model) ระบบบล็อกเชน (Thoppae & Jirawichitchai, 2020) เพื่อใช้ในการจัดเก็บข้อมูลผู้กระทำความผิดในประเทศไทย ทั้งนี้โดยคำนึงถึงความสอดคล้องกับร่างพระราชบัญญัติทะเบียนประวัติอาชญากรรมฯ ซึ่งสำนักงานกิจการยุติธรรม กระทรวงยุติธรรม กำลังดำเนินการจัดทำ พร้อมนำข้อห่วงใยในด้านต่าง ๆ เช่น ด้านความมั่นคงปลอดภัย ด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านความยุติธรรม และด้านความถูกต้องเหมาะสม มาพิจารณาประกอบ

การสัมมนาระดมความเห็น

ผลการศึกษาวิจัย การสำรวจ และการพัฒนาแบบจำลองบล็อกเชนในการจัดเก็บข้อมูลประวัติอาชญากรรมในประเทศไทย ได้ผ่านการนำเสนอและระดมความเห็นจากผู้ที่มีส่วนเกี่ยวข้องในกระบวนการยุติธรรมและผู้เชี่ยวชาญด้านบล็อกเชน แล้วนำข้อเสนอมาปรับปรุงผลการศึกษา ทั้งนี้ได้มีการจัดประชุมสัมมนาวิพากษ์โดยผู้เชี่ยวชาญและผู้มีส่วนเกี่ยวข้องเฉพาะกลุ่ม (focus group) 2 รอบ โดยผู้มีส่วนเกี่ยวข้องได้แก่ ตัวแทนจากสำนักงานตำรวจแห่งชาติ ศาลยุติธรรม สำนักงานอัยการสูงสุด กรมพินิจและคุ้มครองเด็กและเยาวชน กรมคุมประพฤติ และกรมราชทัณฑ์ ศูนย์แลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม (Data Exchange Center : DXC) สำนักงานกิจการยุติธรรม สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สำนักงานธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) บริษัท กสทโทรคมนาคม จำกัด (มหาชน) ธนาคารแห่งประเทศไทย ธนาคารพาณิชย์ ภาคการศึกษา และบริษัทผู้ให้บริการด้านบล็อกเชน

การพัฒนาตัวแบบจำลองด้วยบล็อกเชนสำหรับการจัดเก็บข้อมูลประวัติอาชญากรรม และบูรณาการกระบวนการยุติธรรมในประเทศไทย

หน่วยงาน และภาคส่วนที่เกี่ยวข้องในกระบวนการยุติธรรมทางอาญา ได้แก่

1) พนักงานสอบสวนหรือตำรวจ เป็นหน่วยงานแรกที่รับผิดชอบต่อกระบวนการยุติธรรมก่อนที่คดีหรือข้อพิพาทที่เกิดขึ้น โดยจะมีการส่งผ่านคดีไปยังพนักงานอัยการ และเข้าสู่การพิจารณาของศาล ตำรวจเป็นผู้จับกุมผู้กระทำความผิด และรวบรวมพยานหลักฐานที่ได้จากการสอบสวนแล้วส่งเรื่องหรือสำนวนสอบสวนให้พนักงานอัยการ

2) ทนายความ ดำเนินการว่าความแก้ต่างให้แก่คู่ความไม่ว่าจะเป็นโจทก์หรือจำเลย ทนายความเป็นผู้ประกอบอาชีพกฎหมายโดยอิสระ ทนายความจะให้คำปรึกษาหรือดำเนินคดีแทน โดยคิดค่าบริการจากลูกความ

3) พนักงานอัยการ เป็นเจ้าหน้าที่ของรัฐซึ่งดำเนินคดีต่อจากพนักงานสอบสวน เมื่อพนักงานสอบสวนได้สอบสวนคดีเสร็จแล้วก็จะส่งสำนวนการสอบสวนให้พนักงานอัยการเพื่อฟ้องผู้ต้องหาต่อศาลต่อไป

4) ศาลยุติธรรมเป็นเจ้าหน้าที่ของรัฐ ซึ่งดำเนินคดีต่อจากพนักงานอัยการ เมื่อพนักงานอัยการเห็นสมควรสั่งฟ้องจะส่งฟ้องต่อศาล

5) เจ้าหน้าที่ฝ่ายราชทัณฑ์ ทำหน้าที่ควบคุมผู้ต้องหาหรือจำเลยไว้ในระหว่างการดำเนินคดีอาญาไม่ว่าจะเป็นชั้นก่อนศาลพิจารณา ระหว่างการพิจารณาตลอดจนภายหลังการพิจารณาพิพากษา

จากการศึกษาได้พบปัญหาต่าง ๆ ในกระบวนการยุติธรรมโดยจำแนกปัญหาออกเป็น 4 กลุ่ม โดยมีประเด็นพอสังเขปดังนี้

1. กระบวนการยุติธรรมชั้นสอบสวน (พนักงานสอบสวน และพนักงานอัยการ) เป็นกระบวนการแรก ๆ ที่มีการจัดเก็บหลักฐานในการดำเนินคดี มีประเด็นปัญหาเกี่ยวข้องกับประสิทธิภาพในกระบวนการยุติธรรมชั้นสอบสวน มีปัญหาความไม่เป็นกลาง และความไม่เป็นอิสระของพนักงานสอบสวนในการดำเนินคดี หรืออาจมีการแทรกแซงการสอบสวนคดี ตลอดจนถึงการคุ้มครองสิทธิ และเสรีภาพของผู้ต้องหา การบิดเบือนหรือปลอมแปลงข้อมูลหลักฐานพยานสามารถกระทำได้ง่าย

2. กระบวนการยุติธรรมชั้นศาล ปัญหาหลักได้แก่ โอกาสในการตกเป็นจำเลยในคดีอาญา ระยะเวลาที่ต้องอยู่ในการพิจารณาคดีอาญาตั้งแต่เริ่มคดีจนคดีถึงที่สุด ระยะเวลาที่ต้องอยู่ในการพิจารณาคดีอาญาในแต่ละชั้นศาล ความไม่เสมอภาคจากการกำหนด และบังคับโทษปรับ การพิจารณาคดีอาญาไม่มีความต่อเนื่อง การรับฟังและชั่งน้ำหนักพยานหลักฐานยังมีข้อบกพร่อง การใช้ดุลพินิจในการกำหนดโทษการคุ้มครองพยานบุคคลในคดีอาญายังไม่เป็นธรรม

3. กระบวนการยุติธรรมชั้นบังคับคดี ปัญหาผู้ต้องขังล้นเรือนจำ เจ้าหน้าที่มีไม่เพียงพอต่อการดำเนินงาน ปัญหาเกี่ยวกับการได้รับสิทธิของผู้ต้องขัง ปัญหาด้านข้อมูลที่ไม่ถูกต้อง และเป็นปัจจุบัน

4. กระบวนการยุติธรรมกระแสหลักเป็นการดำเนินคดีโดยองค์กรของรัฐ กระบวนการยุติธรรมกระแสหลักประกอบด้วยการทำหน้าที่ของตำรวจ อัยการ และศาลยุติธรรม โดยพบปัญหาว่ามีความล่าช้า ประชาชนบางส่วนไม่เชื่อถือในความโปร่งใส่ ความไม่ยุติธรรม ค่าใช้จ่ายสูง และประชาชนยังไม่สามารถเข้าถึงกระบวนการยุติธรรมได้อย่างทั่วถึงและเป็นธรรม

ระบบสารสนเทศที่เกี่ยวข้องในกระบวนการยุติธรรม

หน่วยงานในกระบวนการยุติธรรมของประเทศไทย ได้พัฒนาระบบสารสนเทศเพื่อลดปัญหาอุปสรรค เพิ่มประสิทธิภาพการปฏิบัติงาน และเสริมสร้างความเป็นธรรมให้ทั่วถึงในกระบวนการยุติธรรมอย่างต่อเนื่องเรื่อยมานับหลายสิบปี เนื้อหาในส่วนนี้พยายามสรุปสำรวจความก้าวหน้าของระบบสารสนเทศที่มีการใช้งานในกระบวนการยุติธรรมในปัจจุบัน

1. ระบบศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (Data Exchange Center: DXC)

กระทรวงยุติธรรม โดยสำนักงานกิจการยุติธรรม ได้พัฒนาศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) โดยมีวัตถุประสงค์เพื่อใช้เป็นศูนย์กลางการเชื่อมโยงข้อมูลระหว่างหน่วยงานในเครือข่ายความร่วมมือกระบวนการยุติธรรม ทำให้การค้นหาข้อมูลที่เกี่ยวกับคดีต่าง ๆ สามารถทำได้อย่างสะดวก รวดเร็ว และมีความครบถ้วน ทั้งในการตรวจสอบประวัติผู้ที่เกี่ยวข้องหลักฐานเกี่ยวกับคดีตลอดจนสามารถติดตามสถานะของคดีได้อย่างรวดเร็ว และสะดวกในการใช้งานผ่านระบบอินเตอร์เน็ต

2. ระบบ CRIMES ของสำนักงานตำรวจแห่งชาติ (สตช)

ระบบ C.R.I.M.E.S ย่อมาจาก Criminal Record and Information Management

Enterprise Systems เป็นชื่อระบบใหม่ใน “โครงการพัฒนาระบบเทคโนโลยีสารสนเทศสถานีตำรวจ” ที่ได้รับการจัดสรรงบประมาณจากรัฐบาลในปีงบประมาณ 2550-2551 เพื่อสนับสนุนงานของสถานีตำรวจและเป็นระบบที่สามารถเชื่อมโยงฐานข้อมูลของหน่วยงานต่าง ๆ ทั้งในสำนักงานตำรวจแห่งชาติและหน่วยงานพันธมิตรภายนอก เพื่อลดการทำงานซ้ำซ้อนของพนักงานสอบสวนในสถานีตำรวจและหน่วยงานที่มีอำนาจสอบสวนภายใต้สำนักงานตำรวจแห่งชาติกว่า 1,400 แห่ง ทั่วประเทศ และเป็นแหล่งรวบรวมข้อมูลการรับแจ้งเหตุ ข้อมูลเกี่ยวกับคดี ช่วยในการสืบสวนสอบสวน ป้องกันปราบปรามอาชญากรรม และรองรับการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรม โดยจำแนกผู้ใช้เป็น 5 กลุ่ม ได้แก่

1) พนักงานสอบสวน ผู้ช่วยพนักงานสอบสวน หรือเจ้าหน้าที่ประจำสถานีที่ติดตั้งเครื่องคอมพิวเตอร์ลูกข่าย ผู้มีหน้าที่บันทึกหรือเพิ่มเติมข้อมูลอาชญากรรมให้ถูกต้อง

2) เจ้าหน้าที่ตำรวจ ผู้มีหน้าที่ด้านสืบสวนป้องกันและปราบปราม ที่ต้องใช้ข้อมูลในการดำเนินงาน

3) เจ้าหน้าที่ตำรวจ ผู้มีหน้าที่บริหารงานที่ต้องใช้ข้อมูลอาชญากรรมในด้านงานสถิติ

4) เจ้าหน้าที่ตำรวจประจำกองทะเบียนประวัติอาชญากร ผู้มีหน้าที่ตรวจสอบ ยืนยันประวัติผู้ต้องหาลายพิมพ์นิ้วมือ ภาพถ่าย และหมายจับ

5) เจ้าหน้าที่เทคนิค ผู้มีหน้าที่ด้านเทคนิคในการดำเนินการ บำรุงรักษาระบบ ให้สามารถทำงานได้ตลอดเวลา

3. ระบบทะเบียนประวัติผู้กระทำความผิดและระบบตรวจสอบลายพิมพ์นิ้วมืออัตโนมัติ (Automated Fingerprint Identification System: AFIS)

ระบบตรวจสอบลายพิมพ์นิ้วมืออัตโนมัติ (Automated Fingerprint Identification System: AFIS) เป็นการนำเทคโนโลยีคอมพิวเตอร์มาใช้งานร่วมกับหลักวิชาลายพิมพ์นิ้วมือ โดยในขั้นตอนของการใช้งานนั้น ลายพิมพ์นิ้วมือของอาชญากรทั่วประเทศถูกส่งมาตรวจสอบและจัดเก็บในฐานข้อมูลของระบบ AFIS และมีระบบทะเบียนประวัติผู้กระทำความผิดของกองทะเบียนประวัติอาชญากร สตช. ด้วย

จุดลักษณะของลายเส้นของนิ้วมือ และการคำนวณค่าความสัมพันธ์ของจุดต่าง ๆ เป็นค่าทางคณิตศาสตร์สามารถถูกประมวลผลโดยอัตโนมัติ ประเภทลายนิ้วมือ และค่าทางคณิตศาสตร์ของลายนิ้วมือแต่ละนิ้วจะเป็นข้อมูลเข้าไปค้นหาเปรียบเทียบกับฐานข้อมูลในระบบ AFIS หากพบข้อมูลที่ตรงกันแสดงว่าผู้นั้นเคยมีประวัติอาชญากร เพื่อที่จะให้รายละเอียดและยืนยันประวัติทั่วไปของผู้ต้องหา ดังในกรณีสถานที่เกิดเหตุพบลายนิ้วมือแฝง คือ ลายนิ้วมือของผู้ต้องสงสัยไม่สมบูรณ์ ระบบ AFIS สามารถนำลายนิ้วมือที่ไม่สมบูรณ์มาวิเคราะห์หาจุดลักษณะสำคัญ ๆ ของลายเส้นมาสืบค้นกับข้อมูลประวัติอาชญากรได้ เป็นต้น

4. ระบบสารบบคดีของสำนักงานอัยการสูงสุด (Attorney General Office: AGO)

ระบบนี้ใช้จัดเก็บข้อมูลเกี่ยวกับคดี และแลกเปลี่ยนข้อมูลสืบสวนคดีระหว่างสำนักงานตำรวจแห่งชาติในรูปแบบข้อมูลอิเล็กทรอนิกส์

เริ่มตั้งแต่จุดที่พนักงานสอบสวนส่งสำนวนคดีหรือที่มีการร้องขอให้แก้ต่างมายังสำนักงานอัยการสูงสุด การตรวจสำนวนคดี การดำเนินคดีในศาลชั้นต้น ศาลอุทธรณ์ และศาลฎีกา การจัดทำรายงานต่าง ๆ ตลอดจนสถิติเกี่ยวกับคดี ซึ่งมีการจัดเก็บข้อมูลในลักษณะเว็บเทคโนโลยี โดยมีการจัดเก็บข้อมูลแบบรวมศูนย์อยู่ที่ส่วนกลาง การจัดเก็บข้อมูลเป็นลักษณะแบบตอบสนองทันที (real time) มีการประมวลผลเพื่อจัดทำรายงานในช่วงเวลากลางคืนในทุก ๆ คืน มีการสำรองข้อมูลแบบเต็มรูปแบบ (full backup) ทุกวันในรูปแบบของเทป (tape backup) และอุปกรณ์จัดเก็บข้อมูลขนาดใหญ่ พร้อมทั้งให้มีการกำหนดสิทธิในการเข้าถึงข้อมูลตามสิทธิของผู้ใช้งานที่ได้รับในแต่ละระดับด้วย

5. ระบบ Smart Court ของสำนักงานศาลยุติธรรม

ศาลยุติธรรมได้ใช้เทคโนโลยีสารสนเทศสนับสนุนการทำงานในหลายมิติ เช่น การบันทึกคำพยานการสืบค้นเอกสาร การยื่นคำฟ้องที่เป็นอิเล็กทรอนิกส์ (e-Filing) ผ่านทางอินเทอร์เน็ตโดยไม่ต้องใช้กระดาษ ศาลฎีกาใช้เทคโนโลยีสารสนเทศสำหรับระบบสืบค้นทำให้ค้นหาคำพิพากษาศาลฎีกาได้รวดเร็วขึ้น ศาลอุทธรณ์คดีชำนาญพิเศษได้นำเทคโนโลยีสารสนเทศมาพัฒนากระบวนการตรวจร่างคำพิพากษาโดยการใช้โปรแกรมเอดิเตอร์ในการติดตามการแก้ไขเปลี่ยนแปลงไฟล์เอกสาร (track changes) ทำให้ลดขั้นตอนการทำงานและประหยัดทรัพยากรได้อย่างมาก

6. ระบบสารสนเทศกรมคุมประพฤติ (Department of Probation Information System: DOPIS) ของกรมคุมประพฤติ

ระบบนี้เป็นการจัดทำฐานข้อมูลทะเบียนคดีโดยแบ่งตามภารกิจงาน ประกอบด้วยงานคุมประพฤติ งานฟื้นฟูสมรรถภาพผู้ติดยาเสพติด งานกิจกรรมชุมชน และงานสงเคราะห์ผู้กระทำผิด มีการจัดเก็บข้อมูลในรูปแบบรวมศูนย์ และเปิดให้บริการแก่ผู้ใช้งานแบบออนไลน์เรียลไทม์ และรวบรวมข้อมูลการคุมความประพฤติของผู้กระทำผิดในประเทศไทยจากหลายหน่วยงาน จำแนกตามกลุ่มเป้าหมาย เช่น เด็ก ผู้ต้องหา ผู้ต้องโทษจำคุก ซึ่งมีทั้งกรมราชทัณฑ์ กรมพินิจและคุ้มครองเด็กและเยาวชน และกรมคุมประพฤติ ผู้ใช้งานส่วนใหญ่เป็นผู้ปฏิบัติงานในสำนักงานคุมประพฤติซึ่งเป็นผู้นำเข้าข้อมูลโดยตรง และใช้เป็นฐานข้อมูลหลักในการปฏิบัติงานด้านคดีของกรมคุมประพฤติ ทั้งนี้ รายการข้อมูลที่จัดเก็บประกอบด้วยรายการต่าง ๆ อาทิ ประวัติส่วนตัว ข้อมูลทั่วไป ข้อมูลคดี รายงานความเห็น ผลคำพิพากษา เป็นต้น

เทคโนโลยีบล็อกเชนในกระบวนการยุติธรรม

1. เทคโนโลยีบล็อกเชน

บล็อกเชนเป็นเทคโนโลยีที่ใช้วิทยาการการเข้ารหัส (cryptography) ที่ช่วยทำให้ผู้เกี่ยวข้องสามารถทำธุรกรรมหรือข้อตกลงระหว่างกันได้ด้วยความน่าเชื่อถือ (สำนักงานพัฒนารัฐบาล

ดิจิทัล, 2562) ทั้งนี้เนื่องจากรายการธุรกรรมที่ได้ตกลงและกระทำไว้ร่วมกันถ้าได้บันทึกเก็บไว้แล้วนั้นจะไม่สามารถแก้ไขให้ผิดเพี้ยนไปจากเดิมได้ง่าย เช่น เมื่อข้อมูลได้ถูกบันทึกและจัดเก็บไว้แล้ว จะไม่สามารถถูกแก้ไขได้โดยผู้เกี่ยวข้องแต่ละฝ่ายไม่ได้รับรู้ไม่ได้ เป็นต้น ความน่าเชื่อถือที่กล่าวถึงเกิดขึ้นจากกลไก 3 ด้านหลัก คือ การเข้ารหัสลับของข้อมูลในบล็อกเชน กลไกการตรวจสอบความถูกต้องและเห็นชอบร่วมกันของธุรกรรมและข้อมูลที่จะเพิ่มขึ้นในบล็อกเชน (consensus/validation mechanism) และการจัดเก็บหลักฐานหรือบัญชีรายการข้อมูลบล็อกเชนแบบกระจาย (distributed ledgers) กล่าวคือ การจัดเก็บข้อมูลเดียวกันไว้ในหลายแห่ง แต่ข้อมูลที่เก็บต่างที่กันนั้นจะถูกต้องตรงกันเสมอ

2. การประยุกต์บล็อกเชนในระดับสากล

ปัจจุบันเทคโนโลยีบล็อกเชนถูกนำมาประยุกต์ใช้ในเงินสกุลดิจิทัล บิตคอยน์ (bitcoin) เป็นสกุลเงินดิจิทัลที่เป็นการประยุกต์เทคโนโลยีบล็อกเชนแอปพลิเคชันแรกของโลก ทั้งนี้เนื่องจากเทคโนโลยีบล็อกเชนมีศักยภาพในการจัดเก็บและถ่ายโอนกรรมสิทธิ์หรือสินทรัพย์ในลักษณะอื่น ๆ ได้ด้วย เช่น ตราสารเกี่ยวกับการเงิน เอกสารแสดงสิทธิ์ในลักษณะต่าง ๆ โฉนดที่ดิน หลักทรัพย์ ดนตรี ศิลปะ หลักฐานพยาน การค้นพบทางวิทยาศาสตร์ ทรัพย์สินทางปัญญา และแม้กระทั่งการออกเสียงเลือกตั้ง นอกจากนี้เทคโนโลยีบล็อกเชนยังถูกประยุกต์ใช้กับการทำสัญญาอัจฉริยะ (smart contract) ซึ่งคือ โปรแกรมคอมพิวเตอร์ที่สามารถดำเนินการตามข้อตกลงอย่างอัตโนมัติทันทีที่เกิดเหตุการณ์ตามเงื่อนไขในสัญญา ซึ่งได้มีการระบุเงื่อนไขสำหรับรองรับเหตุการณ์ต่าง ๆ ไว้ล่วงหน้า ทั้งนี้โดยไม่ต้องมีคนกลางหรือองค์กรกลางในการบังคับเงื่อนไขของสัญญา ยกตัวอย่างเช่น การโอนเงินจ่ายค่าลิขสิทธิ์ซอฟต์แวร์อัตโนมัติทันทีที่จำนวนผู้ใช้ถึงระดับที่ตกลงกับเจ้าของลิขสิทธิ์ซอฟต์แวร์ไว้ล่วงหน้า และ การโอนเงินจ่ายค่าโฆษณาบนเว็บไซต์โดยอัตโนมัติในทันทีที่จำนวนคนดูถึงระดับที่ตกลงกับเจ้าของเว็บไว้ล่วงหน้า เป็นต้น

ตารางที่ 1 ตัวอย่างการประยุกต์บล็อกเชนในกระบวนการยุติธรรมต่างประเทศ

ประเทศ	ระบบที่ประยุกต์บล็อกเชน	ผู้ที่เกี่ยวข้อง	การประยุกต์เทคโนโลยีบล็อกเชน
เอสโตรเนีย	E-Justice, e-File, e-Law, KSI	ตำรวจ สำนักงานอัยการ ศาล เรือนจำ ศูนย์บริการรัฐ และประชาชน	ด้านกระบวนการยุติธรรม ด้านสุขภาพ และด้านธุรกิจภายในประเทศ
จีน	Chinese Courts and Internet Judiciary	นักเขียน และผู้พิพากษา	ด้านวรรณกรรม และด้านทรัพย์สินทางปัญญา
สวิตเซอร์แลนด์	Jur	หน่วยงานภาครัฐ และภาคเอกชน	ด้านการทำสัญญาอัจฉริยะ และด้านกระบวนการยุติธรรม

3. การประยุกต์บล็อกเชนในกระบวนการยุติธรรม

ในหลายประเทศได้พัฒนา และใช้ประโยชน์จากเทคโนโลยีบล็อกเชนในกระบวนการยุติธรรม กิจการของรัฐในหลายด้าน ดังแสดงตัวอย่างตามตารางที่ 1

ประเทศเอสโตรเนียนับว่าเป็นประเทศแรก ๆ ที่ได้นำเทคโนโลยีบล็อกเชนไปใช้ในการจัดเก็บข้อมูลและเอกสารหลักฐานของหน่วยงานราชการ รวมทั้งหลักฐานประวัติอาชญากรรมในการสอบสวนดำเนินคดีของตำรวจ และกระบวนการชั้นศาล (e-Estonia, 2020; Guardtime, 2020)

ประเทศจีนได้นำบล็อกเชนไปใช้ในการทำหลักฐานพยานแสดงความเป็นเจ้าของวรรณกรรม ส่วนประเทศสวิสเซอร์แลนด์ ได้เริ่มนำเทคโนโลยีบล็อกเชนไปใช้ในขั้นตอนของกระบวนการยุติธรรมด้วยการทำสัญญาอัจฉริยะ (smart contracts) (Supreme People's Court of the People's Republic of China, 2019)

ตัวแบบจำลองบล็อกเชน

1. เป้าหมายในการออกแบบและพัฒนาระบบ

งานวิจัยนี้เสนอการออกแบบ และพัฒนาตัวแบบจำลองเทคโนโลยีบล็อกเชนสำหรับการเชื่อมโยงข้อมูลในกระบวนการยุติธรรม และจัดเก็บข้อมูลประวัติอาชญากรรมสำหรับประเทศไทย โดยมีเป้าหมายการออกแบบ 4 ประการ คือ

1) เพื่อเป็นระบบที่จัดเก็บหลักฐานและประวัติอาชญากรรมในกระบวนการยุติธรรมที่ยากต่อการถูกดัดแปลงโดยมิชอบ

2) เพื่อเพิ่มประสิทธิภาพในการดำเนินการ ลดเวลาและความผิดพลาดในการจัดเตรียมข้อมูล

3) เพื่อช่วยค้นหาและตรวจสอบหลักฐานเป็นศูนย์กลางการค้นหาข้อมูลจากหน่วยงานต่าง ๆ ในกระบวนการยุติธรรม

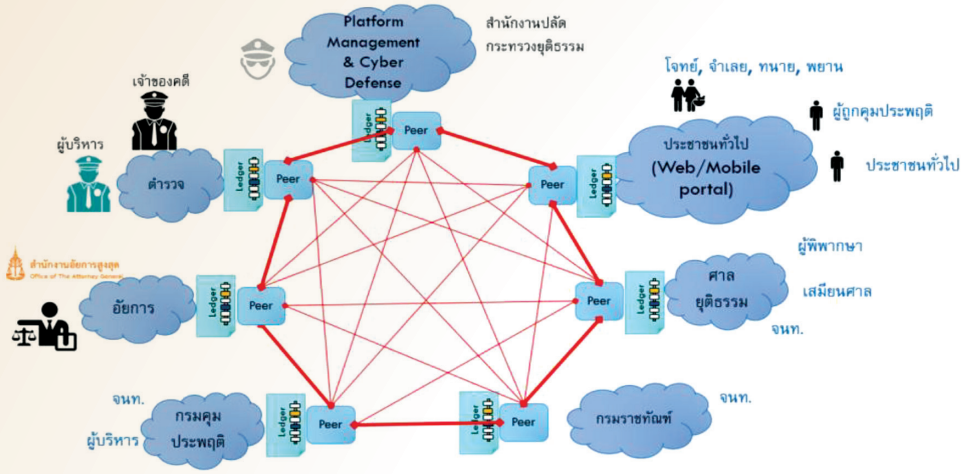
4) เพื่อให้มีความมั่นคงปลอดภัยสูง ที่ยากต่อการเข้าแทรกแซงโดยมิชอบ

การออกแบบสถาปัตยกรรมโดยรวม

ภาพที่ 1 แสดงข้อเสนอการออกแบบสถาปัตยกรรมเครือข่ายบล็อกเชนสำหรับกระบวนการยุติธรรม ด้วยหลักการดังนี้

5) เสนอให้หน่วยงานที่จะพัฒนาและติดตั้งโหนดคอมพิวเตอร์ที่จะเป็น Peers ของเครือข่ายบล็อกเชนเป็นหน่วยงานที่มีส่วนได้ส่วนเสียในกระบวนการยุติธรรมของประเทศไทย โดยเริ่มต้นจาก 3 หน่วยงานแรก คือ สำนักงานตำรวจแห่งชาติ สำนักงานอัยการสูงสุด และสำนักศาลยุติธรรม ทั้งนี้เนื่องจากเป็น 3 หน่วยงานต้นน้ำของข้อมูลหลักฐานต่าง ๆ และประวัติอาชญากรรมในกระบวนการยุติธรรม ส่วนหน่วยงานในลำดับต่อ ๆ ไปที่ควรจะติดตั้งระบบให้เป็น Blockchain Peer Nodes เพิ่มเติมนั้น เมื่อมีความพร้อมทางด้านงบประมาณ และความพร้อมด้านอื่น ๆ อย่างน้อยต้องประกอบด้วยกรมราชทัณฑ์ และกรมคุมประพฤติ

รูปภาพที่ 1 สถาปัตยกรรมเครือข่ายบล็อกเชนสำหรับกระบวนการยุติธรรม



ที่มา: Thoppae & Jirawichitchai, 2020

6) เสนอกำหนดให้มีหน่วยงานหนึ่งทำหน้าที่เป็น **"หน่วยงานอำนวยความสะดวกเครือข่ายบล็อกเชนกระบวนการยุติธรรม"** (Peer Facilitator) ซึ่งเสนอให้เป็นสำนักงานกิจการยุติธรรม โดยมีหน้าที่ส่งเสริม สนับสนุน และประสานงานในเครือข่ายบล็อกเชนในกระบวนการยุติธรรมนี้ ทั้งนี้ หน่วยงานดังกล่าวไม่ได้ทำหน้าที่เป็นศูนย์กลางของระบบ ไม่มีอำนาจในเครือข่ายเหนือหน่วยงานอื่น ๆ แต่ทำหน้าที่ด้านการอำนวยความสะดวก คอยประสานความร่วมมือ ให้ความรู้ทางเทคนิคกับสมาชิกในเครือข่าย สนับสนุนการปรับปรุงเวอร์ชันของซอฟต์แวร์ ทำหน้าที่ตรวจสอบ และป้องกันการทำธุรกรรมแบบไม่ปกติ และให้ความช่วยเหลือทางเทคนิคแก่หน่วยงานในเครือข่ายบล็อกเชนให้สามารถปฏิบัติงานได้ตามมาตรฐานที่พึงปฏิบัติ หน่วยงานดังกล่าวจะต้องมีการพัฒนา และติดตั้งระบบคอมพิวเตอร์ที่เป็น Peer Node ในเครือข่ายนี้ด้วย

7) เสนอหน่วยงานที่จะเชื่อมโยงเข้ากับเครือข่ายบล็อกเชนแต่ละหน่วยงาน พึงต้องมีระบบสารสนเทศอิเล็กทรอนิกส์ที่สนับสนุนพันธกิจหลักภายในตามกระบวนการยุติธรรมที่หน่วยงานนั้นรับผิดชอบ โดย Peer Node ที่จะเชื่อมต่อเข้ากับเครือข่ายบล็อกเชนนี้จะทำหน้าที่เป็นอินเตอร์เฟส (interface) ระหว่างระบบสารสนเทศภายใน

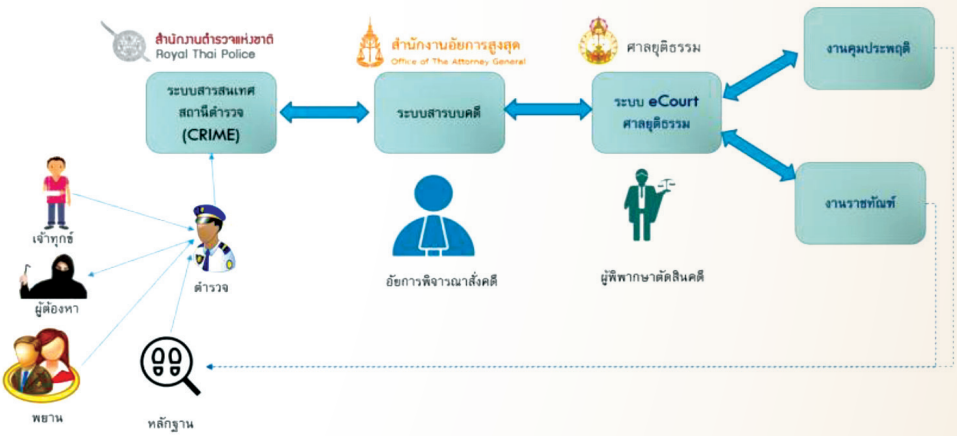
8) การเชื่อมโยงเครือข่ายบล็อกเชนจะเกิดการจัดเก็บข้อมูลหลักฐาน และประวัติอาชญากรรมในรูปแบบธุรกรรมอิเล็กทรอนิกส์กระจายไปพร้อมกันตามโหนดต่าง ๆ ที่มีอยู่ในเครือข่ายทั้งหมด (distributed ledgers) การกระจายการจัดเก็บไปในหลายโหนดของบล็อกเชนนั้นจะช่วยให้การจัดเก็บข้อมูลหลักฐานสามารถยืนยันความถูกต้องตรงกันจากหลาย ๆ โหนดนั้น ซึ่งจะส่งผลให้ต้องมีการยืนยันข้อมูลหลักฐานเหล่านั้นในระบบต้องถูกต้องตรงกัน และไม่ให้

เกิดการแก้ไข หรือบิดเบือนข้อเท็จจริง ทำให้เกิดการทุจริตได้ยาก

3. กระบวนการหลักของการดำเนินคดี

ผังการไหลของข้อมูลหลักในการดำเนินคดีแสดงดัง ภาพ 2 สังเกตในส่วนของระบบสารสนเทศของแต่ละหน่วยงานนั้นจะได้รับการพัฒนาอย่างเป็นอิสระจากหน่วยงานอื่น อาทิ ระบบเทคโนโลยีสารสนเทศสถานีตำรวจ (CRIMES) ถูกพัฒนาขึ้นเพื่อตอบสนองความต้องการของสถานีตำรวจ ระบบสารบบคดีอิเล็กทรอนิกส์ได้มีการถูกพัฒนาขึ้นเพื่อตอบโจทย์ความต้องการของสำนักงานอัยการสูงสุด เช่นเดียวกันกับระบบ Smart Court ถูกสร้างตามเงื่อนไขความต้องการของศาลยุติธรรม เป็นต้น (ISECT, 2012)

รูปภาพที่ 2 กระบวนการดำเนินคดี และการเชื่อมโยงระหว่างระบบสารสนเทศของหน่วยงานที่เกี่ยวข้อง

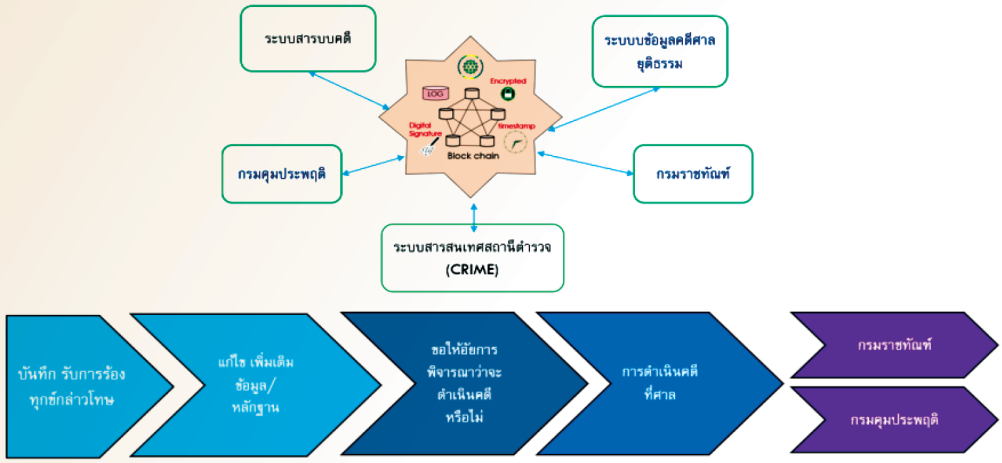


ที่มา: Thoppae & Praneetpolgrang, 2021

การออกแบบระบบเชื่อมโยงในอนาคตจึงมีความต้องการที่จะให้ระบบสารสนเทศทั้งหมดเหล่านั้นสามารถทำงานสัมพันธ์ต่อเนื่องกัน โดยจะต้องมีข้อมูลที่สามารถแลกเปลี่ยนเชื่อมโยงเข้าหากันแบบอัตโนมัติมากขึ้น ทั้งนี้โดยมุ่งหวังให้เกิดการทำงานอย่างสอดคล้อง รวดเร็ว มีประสิทธิภาพในการทำงานร่วมกัน รวมทั้งเพิ่มความถูกต้อง และแก้ปัญหาไม่ให้มีการบิดเบือนหรือไม่ให้มีการแก้ไขปลอมแปลงข้อมูลเป็นสำคัญ

จากขั้นตอนในการดำเนินคดีโดยใช้บล็อกเชนในการเชื่อมระหว่างหน่วยงาน โดยแต่ละหน่วยงานใช้ระบบสารสนเทศที่ใช้งานอยู่ในปัจจุบันเช่นเดิม แต่พัฒนาเพิ่มเติมในส่วนระบบเชื่อมโยงธุรกรรมผ่านเครือข่ายบล็อกเชน ตามภาพที่ 3 แนวคิดนี้ทำให้ไม่จำเป็นต้องพัฒนาระบบสารสนเทศภายในของแต่ละหน่วยงานต่าง ๆ ขึ้นมาใหม่

รูปภาพที่ 3 ขั้นตอนต่าง ๆ ในการดำเนินคดี และระบบสารสนเทศที่เกี่ยวข้อง



ที่มา: Thoppae & Praneetpolgrang, 2021

4. นโยบายการเข้ารหัส

งานวิจัยนี้กำหนดให้มีการเข้ารหัสข้อมูลที่แลกเปลี่ยนกันระหว่างระบบสารสนเทศของหน่วยงานต่าง ๆ ในแพลตฟอร์มนี้ด้วยคุณสมบัติดังต่อไปนี้

1) การเข้ารหัส แบบสมมาตร (symmetric encryption) สำหรับแพลตฟอร์มนี้ ใช้การเข้ารหัสแบบ AES โดยมีความยาวของกุญแจอย่างน้อย 256 บิต (AES-256) หรือการเข้ารหัสแบบอื่นที่สอดคล้องกับมาตรฐาน FIPS 140-2 ที่มีความปลอดภัยของกุญแจไม่น้อยกว่า AES-256

2) Hash function ที่ปลอดภัย ใช้อัลกอริทึม SHA-2 หรือ SHA-3 ที่มีความยาวของกุญแจอย่างน้อย 256 bits หรืออัลกอริทึมอื่นที่ปลอดภัยกว่า

3) การแลกเปลี่ยนกุญแจ ซอฟต์แวร์ที่พัฒนาขึ้นเพื่อใช้ในแพลตฟอร์มนี้จะต้องไม่ส่งรหัสผู้ใช้และ/หรือรหัสผ่านข้ามระบบเครือข่ายแบบ plain text โดยที่การแลกเปลี่ยนกุญแจต้องใช้อัลกอริทึม Diffie-Hellman หรือ IKE หรือ ECDH

4) การสร้างกุญแจ (Key Generation) สำหรับใช้ด้านความปลอดภัย (Cryptographic key) ในโครงการนี้ ต้องใช้ฟังก์ชันการสุ่มที่ปลอดภัย (RNG) ที่สอดคล้องกับประกาศ NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2

5. การเข้ารหัสการเชื่อมต่อแบบ Trusted path

การเชื่อมต่อระหว่างผู้รับ และผู้ส่งในแพลตฟอร์มนี้ ต้องใช้การเชื่อมต่อผ่าน “เส้นทางที่ไว้วางใจได้ (trusted path)” ซึ่งการเชื่อมต่อนั้นจะต้องเป็นเส้นทางเฉพาะตัว ผู้อื่นต้องไม่สามารถจะรับรู้เนื้อหาข้อมูล ที่สื่อสารกัน และเนื้อหาจะต้องไม่ถูกเปลี่ยนแปลงระหว่างทาง ดังรูปภาพที่ 4 โดยมีคุณสมบัติดังนี้

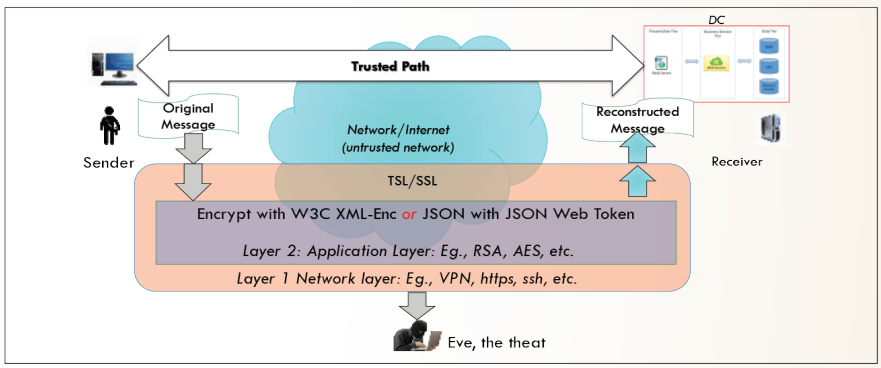
1) การเข้ารหัสระดับระบบเครือข่าย ใช้การเข้ารหัสที่ระบบเครือข่าย ตามนโยบายการเข้ารหัส

โดยใช้มาตรฐาน TLS/SSL, HTTPS ซึ่งจะใช้กุญแจคู่ที่เกิดจากการสร้างโดย Certificate Authority ที่มีความน่าเชื่อถือในการสร้างกุญแจคู่นี้ (Public key และ Private key)

2) การเข้ารหัสระดับแอปพลิเคชัน ใช้กลไกการเข้ารหัสที่แอปพลิเคชันตามนโยบายการเข้ารหัส โดยใช้มาตรฐาน W3C XML Encryption Syntax and Processing (XML-ENC) สำหรับข้อมูลแบบ XML หรือมาตรฐาน JSON Web Token (RFC 7519) สำหรับข้อมูลแบบ JSON

3) กรณีการเข้ารหัสแบบ XML ให้ดูรูปภาพแบบข้อที่ 7

รูปภาพที่ 4 การสร้าง Trusted path ของแพลตฟอร์ม

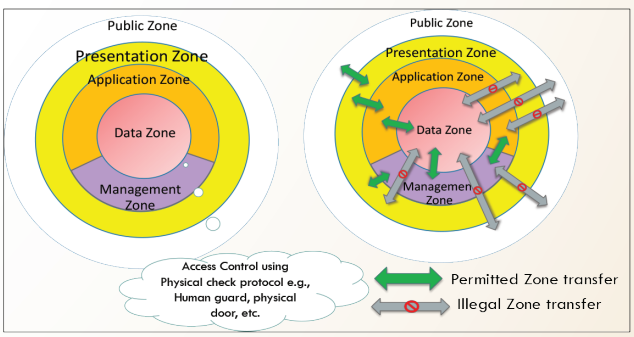


ที่มา: Chaisuriya, Keretho, Sanguanpong and Thoppae, 2021

6. เครือข่ายของศูนย์สารสนเทศแบบวงแหวน

งานวิจัยกำหนดการออกแบบและติดตั้งคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ในศูนย์สารสนเทศของแพลตฟอร์มนี้ โดยใช้โทโปโลยีเครือข่ายแบบวงแหวนหลายชั้น (defense in depth) (Chaisuriya, Keretho, Sanguanpong, & Thoppae, 2021) สถาปัตยกรรมเครือข่ายแบบวงแหวนหลายชั้น ดังแสดงในรูปภาพที่ 5

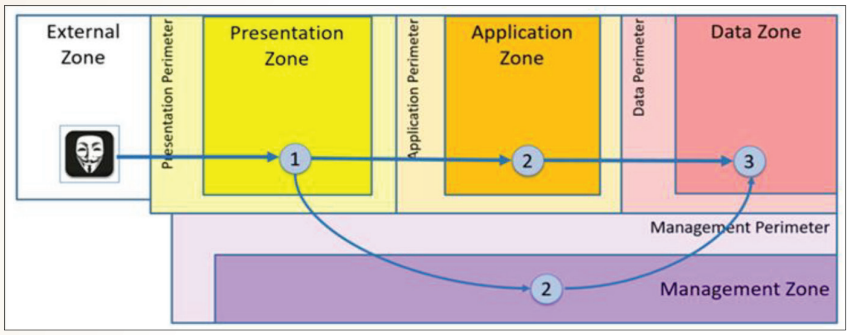
รูปภาพที่ 5 สถาปัตยกรรมเครือข่ายแบบวงแหวนหลายชั้น และข้อกำหนดในการสื่อสารข้ามโซน



ที่มา: Chaisuriya, Keretho, Sanguanpong and Thoppae, 2021

เครือข่ายแบบวงแหวนหลายชั้น และข้อกำหนดในการสื่อสารข้ามโซน ซึ่งเป็นการใช้หลักการป้องกันเชิงลึก (defense in depth) ที่กำหนดให้การข้อถึงข้อมูลหลักของระบบจะต้องผ่านแนวป้องกันหลายชั้น กำหนดให้ใช้จำนวนแนวป้องกัน 3 ชั้น โดยแบ่งขอบเขตย่อย ๆ ในระบบออกเป็น “โซน” แต่ละโซน ประกอบไปด้วยคอมพิวเตอร์และอุปกรณ์เครือข่ายที่สามารถเชื่อมต่อถึงกัน (Routable Network) เรียกขอบของโซนว่า “Perimeter” ซึ่งประกอบได้ด้วยอุปกรณ์การเชื่อมต่อและระบบป้องกันโซน (อาทิ Firewall, IPS/IDS) โดยสามารถแสดงรูปที่ 6 และให้มีข้อกำหนด “ด้านโมเดลการโจมตี” ในการเข้าถึงข้อมูลใน Data Zone จะต้องผ่านการข้ามโซนอย่างน้อย 3 ครั้งเสมอในทุกทิศทาง (Chaisuriya, Keretho, Sanguanpong, & Praneetpolgrang, 2018) ดังแสดงในรูปภาพที่ 6

รูปภาพที่ 6 ข้อจำกัดการเข้าถึงข้อมูลใน Data Zone



ที่มา: Chaisuriya, Keretho, Sanguanpong and Praneetpolgrang, 2018

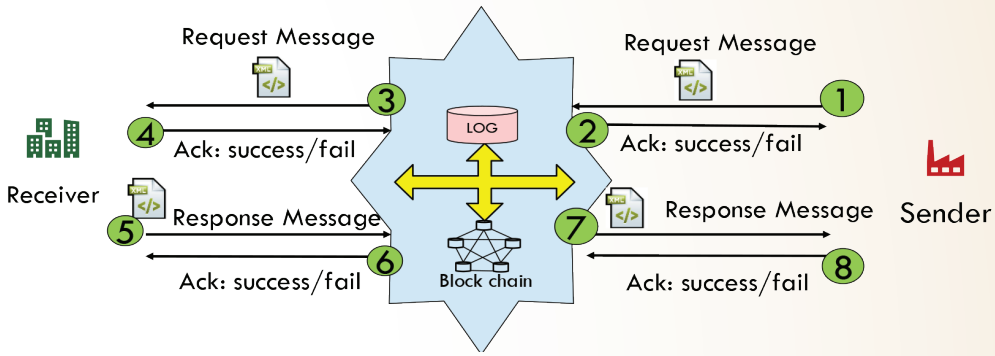
7. มาตรฐานการเชื่อมข้อมูลของแพลตฟอร์ม

กำหนดให้การรับส่งข้อมูลพื้นฐานของแพลตฟอร์มใช้การรับส่งข้อมูลแบบ Asynchronous ผ่านแพลตฟอร์มดังแสดงใน รูปภาพที่ 7 โดยที่

1) ในการส่งข้อมูลผู้ส่งต้องส่งข้อมูลในรูปแบบที่กำหนด ให้แก่ ส่วนให้บริการ รับส่งข้อมูลของแพลตฟอร์ม (ตามขั้นที่ 1, 2 ในภาพที่ 7) ซึ่งจะได้คำตอบจากส่วนให้บริการนั้นว่า “สำเร็จ” หรือ “ล้มเหลว” ในทันที แต่ทั้งนี้มิใช่คำตอบจากผู้รับข้อมูลปลายทาง เมื่อเวลาผ่านไประยะหนึ่งหลังจาก ส่วนให้บริการรับส่งข้อมูลของแพลตฟอร์ม ได้รับคำตอบจากปลายทางแล้ว ผู้ส่งข้อมูลจึงจะได้รับคำตอบ (ขั้นที่ 7, 8 ในรูปภาพที่ 7)

2) ส่วนผู้รับข้อมูล กระทำในลักษณะเดียวกันตามขั้นที่ 3, 4 และ 5, 6 ดังแสดงในรูปภาพที่ 7

รูปภาพที่ 7 การรับ/ส่งข้อมูลแบบ Asynchronous

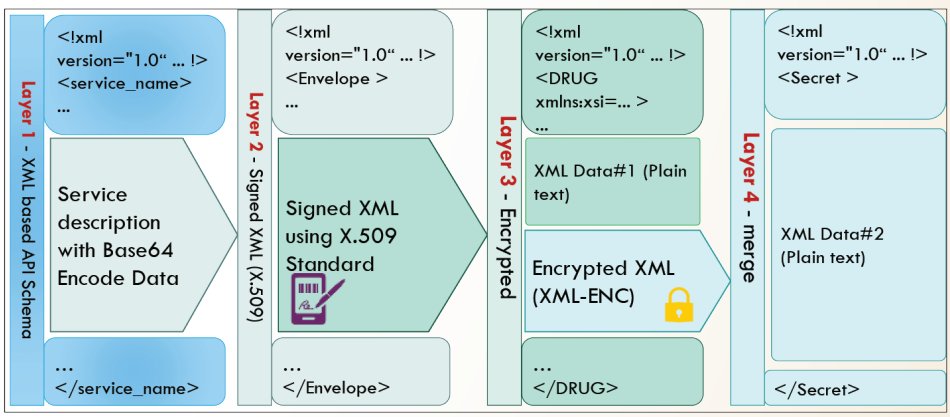


ที่มา: Thoppae and Jirawichitchai, 2020

8. มาตรฐานข้อมูลแบบ XML

รูปแบบของเอกสารที่แลกเปลี่ยนกันในระบบ จะแบ่งออกเป็นชั้น (layer) ต่าง ๆ ทั้งหมด 4 ชั้น (Thoppae, 2021) ดังแสดงในรูปภาพที่ 8

รูปภาพที่ 8 รูปแบบของข้อมูลและการเข้ารหัสข้อมูลแบบ 4 ชั้น ตามมาตรฐานข้อมูลแบบ XML ที่ใช้ในแพลตฟอร์ม



ที่มา: Thoppae and Jirawichitchai, 2020

Layer 4 เป็นข้อมูลที่สำคัญที่สุด ใน Layer นี้ระบบจะจัดเตรียมข้อมูลในรูปแบบ XML สำหรับข้อมูลหลักที่ต้องการส่ง โดยเข้ารหัสด้วยกุญแจคู่ชุด แล้วนำไปใส่ไว้ในส่วนข้อมูลของชั้นที่ 3 ต่อไป

Layer 3 เป็นข้อมูลที่ไม่ต้องเข้ารหัส ซึ่งชั้นที่ 3 นี้จะนำข้อมูลจากชั้นที่ 4 ที่ถูกเข้ารหัสมาประกอบเพื่อจัดเตรียมข้อมูลแบบ base 64 encoding สำหรับชั้นที่ 2 ต่อไป

Layer 2 เป็นชั้นที่นำข้อมูลจากชั้นที่ 3 มาเพื่อลงลายมือชื่อแบบอิเล็กทรอนิกส์ ในขั้นตอนนี้จะได้ลายมือชื่อแบบอิเล็กทรอนิกส์ออกมาเพื่อยืนยันตัวตนทางอิเล็กทรอนิกส์ และจัดเตรียมข้อมูลแบบ base64 สำหรับชั้นที่ 1 ต่อไป

Layer 1 เป็นชั้นสุดท้ายที่นำข้อมูลจากชั้นที่ 2 มีการจัดเตรียมเป็นรูปแบบ Base64 Encoding แล้วส่งออกไปทางช่องทาง SSL/TSL ซึ่งประกอบกันเป็นช่องทางการเชื่อมต่อที่เราเรียกว่า Trusted Path

9. การส่งแฟ้มข้อมูลขนาดใหญ่

กรณีการส่งแฟ้มขนาดใหญ่ กำหนดให้ใช้กลไก ดังแสดงในภาพที่ 9

1) ใช้การรับส่งแบบ Asynchronous โดยไม่ผ่านบล็อกเชน

2) ผู้ส่งแฟ้ม ต้องตัดแฟ้ม (ขนาดใหญ่) ให้เป็นแฟ้มขนาดเล็กหลายแฟ้ม ที่ไม่ใหญ่เกินกว่าการรับส่งแบบ RESTful ด้วยความเร็วช่องทางสื่อสารทั่วไป (เช่น 10 Mbps) จะรองรับได้ อาทิ ขนาด 1 Mbyte (ผู้ใช้สามารถเลือกขนาดของแฟ้มขนาดเล็กที่เหมาะสมกับความเร็วของช่องทางการสื่อสารที่มีอยู่ได้) จากนั้นส่งรายละเอียดของแฟ้มขนาดใหญ่ (ประกอบด้วย ชื่อแฟ้ม รหัส Hash ขนาด ชนิด เป็นต้น) ขนาด/จำนวน/รหัส hash ของแฟ้มขนาดเล็ก ให้ผู้รับข้อมูล

3) ผู้ส่งทยอยส่งแฟ้มขนาดเล็กทั้งหมดเข้าสู่แพลตฟอร์ม

4) ผู้รับทยอยรับแฟ้มทีละแฟ้ม และทยอยแจ้งผล (สำเร็จ หรือ ล้มเหลว) การรับแฟ้มขนาดเล็กแต่ละแฟ้ม

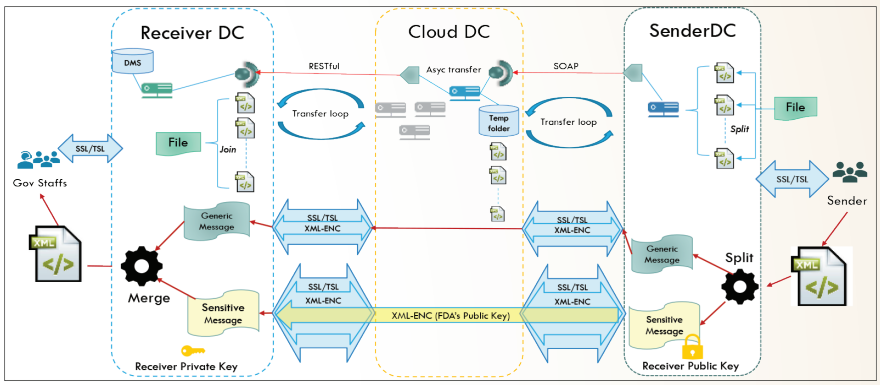
5) กรณีที่แฟ้มขนาดเล็กแฟ้มใด ประสบปัญหาในการรับ/ส่งข้อมูล ให้ผู้ส่งข้อมูล ส่งแฟ้มนั้นใหม่ได้

6) กรณีที่ผู้รับข้อมูล ได้รับแฟ้มทั้งหมดเรียบร้อยแล้ว ให้ดำเนินการ รวมข้อมูลจากแฟ้มเล็กทุกชิ้นให้เป็นแฟ้มใหญ่ต้นฉบับ แล้วแจ้งผลการดำเนินการให้ ผู้ส่งข้อมูล

7) กรณีที่การส่งแฟ้มทั้งหมดใช้เวลานานเกินไป หรือ เกิดข้อผิดพลาดในการส่งมากเกินไป (อาทิ ระบบสื่อสารขัดข้อง) ทั้งผู้ส่งและผู้รับสามารถแจ้งยกเลิกได้

8) การบันทึกรายละเอียดของแฟ้มนี้ลงในบล็อกเชนให้กระทำหลังการรับส่งสำเร็จเรียบร้อยแล้ว

รูปภาพที่ 9 การรับและส่งข้อมูลขนาดใหญ่ผ่านเครือข่ายบล็อกเชน

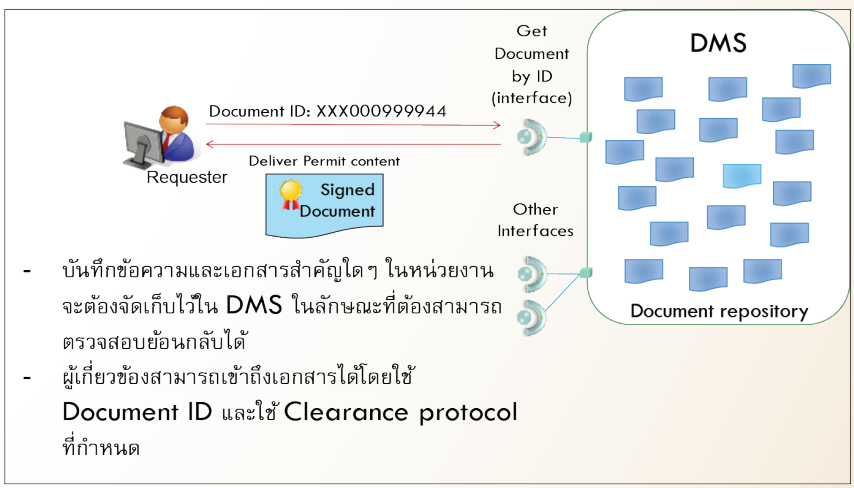


ที่มา: Thoppae and Praneetpolgrang, 2021

10. ระบบการจัดการเอกสาร (Document Management System) ที่ใช้เทคโนโลยีบล็อกเชน

ระบบจัดเก็บเอกสาร (Document Management System: DMS) นี้เป็นระบบที่ใช้ในการควบคุม จัดการ การจัดเก็บเอกสารอิเล็กทรอนิกส์ ของแบบจำลองนี้ ดังแสดงในรูปภาพที่ 10 มีคุณสมบัติดังนี้

รูปภาพที่ 10 ระบบการจัดการเอกสาร (Document Management System)



ที่มา: Thoppae and Jirawichitchai, 2020

1) เป็นระบบที่ติดตั้งบนเครื่องแม่ข่ายใน Data Zone

2) ใช้ระบบจัดการฐานข้อมูลในการทำทะเบียนเอกสาร โดยแฟ้มใหญ่ที่สุดที่จัดเก็บได้จะต้องไม่น้อยกว่า 10 GB

3) รองรับเอกสารต้นฉบับหลายรูปแบบ (format) ดังนี้ XML, JSON, MS-Word, PDF, JPG, TIFF, Excel, Power Point, AVI, MP3, MP4, ZIP, CSV, Text และรูปแบบอื่น ๆ ที่เป็นไฟล์ไบนารี (Binary File) และไฟล์ข้อความ (text file)

4) รองรับการนำแฟ้มขนาดใหญ่ เข้าจัดเก็บในระบบ

5) รองรับการเข้ารหัสเอกสารและการลงลายมือชื่อแบบอิเล็กทรอนิกส์ตามนโยบายการเข้ารหัส

6) กำหนดประเภทของเอกสาร และกำหนดได้ประเภทเอกสารนั้น จะมีข้อมูลลักษณะเฉพาะอะไรบ้าง ข้อมูลลักษณะเฉพาะนี้อาจจะเรียกว่า “แอตทริบิวต์ (Attribute)” โดยพื้นฐานแล้วข้อมูลลักษณะเฉพาะอาจจะมีชนิดเป็นได้ทั้ง ตัวอักษร หรือตัวเลข รวมทั้งมีการนำเอาแอตทริบิวต์ที่มีอยู่แล้วมาประกอบเข้าด้วยกันให้เป็นแอตทริบิวต์ที่ใหญ่กว่า และมีความหมายมากขึ้นได้ สามารถกำหนดได้ว่าเอกสารแต่ละฉบับมีประเภทเอกสารเป็นชุดอะไร พร้อมทั้งระบุค่าของแอตทริบิวต์ที่เพิ่มเติมให้กับเอกสารนั้นได้ ให้กำหนดประเภทเอกสารที่จะนำมาใช้ อย่างน้อย ควรจะต้องมีแอททริบิวท์ได้แก่ ชื่อเอกสาร ประเภทเอกสาร วันที่จัดเก็บเวอร์ชัน หมายเลขเอกสาร ลายมือชื่อแบบอิเล็กทรอนิกส์ ข้อมูลเรื่องการเข้ารหัส เป็นต้น

7) เอกสารมีรหัสที่เป็น Unique ID ของทั้งระบบ

8) มีกลไกการตรวจสอบเอกสารที่มีคุณสมบัติดังนี้

- ตรวจสอบความสมบูรณ์เนื้อเอกสาร
- ตรวจสอบความสอดคล้องกันระหว่างเนื้อหา และลายมือชื่ออิเล็กทรอนิกส์ที่จัดเก็บ
- รองรับทั้งการตรวจสอบแบบเฉพาะเอกสารที่ต้องการตรวจสอบ และการตรวจสอบเอกสาร จำนวนมากทั้งกลุ่ม หรือเอกสารทั้งหมดในระบบ (batch verify)

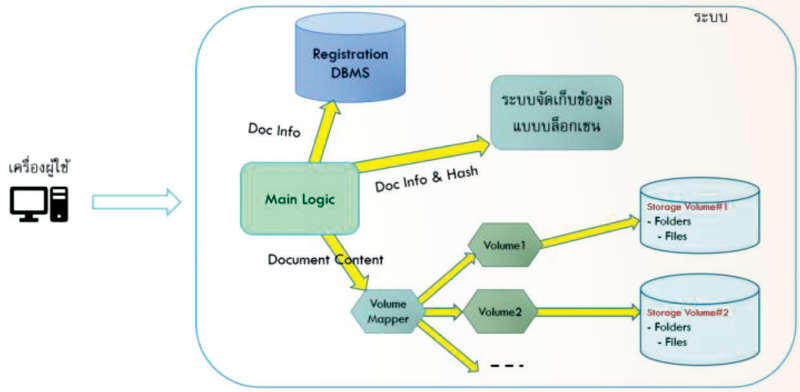
9) ออกแบบให้รองรับการจัดเก็บเอกสารได้อย่างน้อย 1,000 ล้านเอกสาร

10) มี API เชื่อมต่อแบบ Web Service ที่มีคุณสมบัติดังนี้

- API จะต้องรองรับการ Upload ที่ใช้เวลานาน สำหรับกรณีเอกสารขนาดใหญ่ และ/หรือใช้การเชื่อมต่อระบบเครือข่ายความเร็วต่ำ
- กรณีระบบเครือข่ายเกิดข้อผิดพลาด ระบบจะต้องยอมให้ Upload เอกสารต่อ (resume) ได้ ไม่ต้องเริ่มต้นใหม่ หากกลับเข้ามา Resume ภายในระยะเวลาที่กำหนด เช่น ภายใน 15 นาที
- มี API ที่ใช้สำหรับนำเข้าเอกสาร สืบค้นเอกสาร ดาวน์โหลดเนื้อหาเอกสาร เป็นแบบ Web Services
- มี API ที่ใช้จะเชื่อมต่อแบบมีการเข้ารหัสและถอดรหัสของเอกสารอิเล็กทรอนิกส์ระหว่างการรับส่งข้อมูล

เนื่องจากคุณสมบัติของซอฟต์แวร์บล็อกเชนไม่เหมาะสำหรับการเก็บข้อมูลขนาดใหญ่ แพลตฟอร์มนี้จึงเสนอให้เก็บเฉพาะ hash ของเอกสารในบล็อกเชนเท่านั้นดังแสดงในรูปภาพที่ 11

รูปภาพที่ 11 การใช้ Hash ในบล็อกเชนเพื่อควบคุมความถูกต้องของเอกสารใน DMS



ที่มา: Thoppae & Jirawichitchai, 2020

ผลการประชาพิจารณ์

ผลการศึกษาวิเคราะห์และแบบจำลองที่พัฒนาขึ้นนี้ถูกนำเสนอแก่ผู้เชี่ยวชาญด้านเทคโนโลยี บล็อกเชน และวิพากษ์เพื่อรับฟังความคิดเห็นจากผู้เกี่ยวข้องในกระบวนการยุติธรรมในประเด็นหลัก ๆ ดังต่อไปนี้

1. การระดมความคิดเห็นผู้เชี่ยวชาญด้านเทคโนโลยี

1) ผู้เชี่ยวชาญเห็นด้วยว่าสามารถนำเทคโนโลยีบล็อกเชนมาช่วยเพิ่มความโปร่งใส ป้องกันการปลอมแปลง และเพิ่มความน่าเชื่อถือในการจัดเก็บข้อมูลประวัติ อาชญากรรมในประเทศไทย

2) ผู้เชี่ยวชาญเห็นด้วยว่าให้ประยุกต์ใช้บล็อกเชนแบบ Private/Consortium Blockchain ในการจัดเก็บข้อมูลประวัติอาชญากรรมในประเทศไทย

3) ปัจจัยสำเร็จในการประยุกต์เทคโนโลยีบล็อกเชนในการจัดเก็บข้อมูลประวัติอาชญากรรมในประเทศไทยได้แก่ นโยบายและความร่วมมือของหน่วยงาน และเครื่องมือและอุปกรณ์ที่จำเป็น

4) หลักฐานต่าง ๆ ที่ใช้การประกอบการดำเนินคดี เช่น ไฟล์เอกสาร รูปภาพ และวิดีโอ เป็นต้น ที่มิได้ถูกจัดเก็บใน Blockchain (ใน Blockchain เก็บเพียง Hash Value จำนวน 256 bits) ควรมีวิธีการกำกับดูแลห้ามมิให้มีการเปลี่ยนแปลงแก้ไขโดยมิชอบเช่นกัน

5) การพัฒนาบุคคลากรระดับสูง ระดับกลาง ระดับต้นให้มีทัศนะคติความรู้และทักษะที่จำเป็น

2. การวิพากษ์ผลการวิจัยกับผู้ที่เกี่ยวข้องในกระบวนการยุติธรรม

1) ผู้เข้าร่วมประชุมเห็นด้วยว่าสามารถนำเทคโนโลยี Blockchain มาช่วยเพิ่มความ

โปร่งใส ป้องกันการปลอมแปลง และเพิ่มความน่าเชื่อถือ ในการจัดเก็บข้อมูลประวัติอาชญากรรมในประเทศไทย

2) ผู้เข้าร่วมประชุมเห็นด้วยว่าให้ประยุกต์ใช้บล็อกเชนแบบ Private/Consortium Blockchain ในการจัดเก็บข้อมูลประวัติอาชญากรรมในประเทศไทย

3) ปัจจัยสำเร็จในการประยุกต์เทคโนโลยี Blockchain มาใช้ในการจัดเก็บข้อมูล ประวัติอาชญากรรมในประเทศไทยได้แก่

• การคัดเลือกหน่วยงานนำร่อง และกรณีตัวอย่างที่มีขั้นตอนชัดเจน

• ความพร้อมของบุคลากรหน่วยงานที่เห็นด้วยกับการใช้ blockchain อยู่แล้ว เพื่อเปลี่ยนจากการส่งต่อแบบเดิมทีละหน่วยงานมาใช้ blockchain

• งบประมาณ และความรู้ความสามารถของบุคลากร

• การกำหนดหน่วยงาน และกรณีตัวอย่างที่คุ้มค่ากับการลงทุนและใช้งาน blockchain

• ความรู้ของผู้ปฏิบัติรวมกับทัศนคติ

4) หน่วยงานควรเริ่มต้นด้วยการมีธรรมาภิบาลข้อมูลเพื่อให้มีการกำหนดกระบวนการตัดสินใจที่เป็นรูปธรรมชัดเจนว่าจะ Share ข้อมูลได้หรือไม่

5) ผู้ใช้ต้องมีความเข้าใจและเชื่อมั่นในระบบมากพอ

▣ บทสรุปและข้อเสนอแนะ

ผลสรุปของงานวิจัยนี้พบว่า เทคโนโลยีบล็อกเชนมีศักยภาพในการเชื่อมโยงข้อมูลและบูรณาการงานปฏิบัติการระหว่างหน่วยงานในกระบวนการยุติธรรมให้มีความโปร่งใส มีกลไกป้องกันการดัดแปลงข้อมูลหลักฐานโดยมิชอบ ช่วยทำให้การปฏิบัติงานด้านยุติธรรมมีประสิทธิภาพด้วยเทคโนโลยีการเข้ารหัส (cryptography) รวมทั้งมีการบันทึกข้อมูลหลักฐานแบบกระจายและไม่สามารถเปลี่ยนแปลงข้อมูลได้ (immutable distributed ledgers)

1) เสนอให้สำนักงานศาลยุติธรรมทำหน้าที่เป็นนายทะเบียนประวัติอาชญากรรมบล็อกเชน ทั้งนี้ให้เป็นไปตามเงื่อนไขและอำนาจหน้าที่ที่จะกำหนดโดย ร่าง พ.ร.บ. ทะเบียนประวัติอาชญากรรม หรือที่จะเป็นไปตามข้อกำหนดของพระราชบัญญัติฉบับสมบูรณ์ในอนาคต

2) เสนอให้หน่วยงานที่ควรจะพัฒนาและติดตั้ง Blockchain Peers จำนวน 3 หน่วยงานแรก คือ สำนักงานตำรวจแห่งชาติ สำนักงานอัยการสูงสุด และสำนักงานศาลยุติธรรม ทั้งนี้เนื่องจากเป็น 3 หน่วยงานต้นน้ำของข้อมูลหลักฐาน และประวัติอาชญากรรมในกระบวนการยุติธรรม ส่วนหน่วยงานในลำดับต่อไปที่อาจจะมีการติดตั้งคอมพิวเตอร์เป็น Peer เพิ่มขึ้นเมื่อมีงบประมาณ และความพร้อมด้านกำลังคนและระบบสารสนเทศภายใน คือ กรมราชทัณฑ์ และกรมคุมประพฤติ

3) นอกจากนี้ ยังเสนอให้แต่งตั้งหน่วยงานหนึ่งทำหน้าที่เป็น “หน่วยงานอำนวยความสะดวกเครือข่ายบล็อกเชนกระบวนการยุติธรรม” (Peer Facilitators) โดยเสนอให้ “สำนักงานกิจการยุติธรรม” ทำหน้าที่ดังกล่าว โดยมีบทบาทในการส่งเสริม สนับสนุน และประสานงานในเครือข่ายบล็อกเชนในกระบวนการยุติธรรมนี้

4) แต่ละหน่วยงานที่เชื่อมโยงเข้ากับเครือข่ายบล็อกเชนพึงมีระบบสารสนเทศที่สนับสนุนพันธกิจหลักภายในตามกระบวนการยุติธรรมที่หน่วยงานนั้นรับผิดชอบ โดย Peer Node ที่จะเชื่อมต่อเข้ากับเครือข่ายบล็อกเชนนี้จะทำหน้าที่เป็นอินเตอร์เฟสระหว่างระบบสารสนเทศภายในหน่วยงาน กับเครือข่ายบล็อกเชน ทั้งเพื่อให้เกิดการจัดเก็บข้อมูลหลักฐาน และประวัติอาชญากรรมสำคัญ ๆ ซ้ำและกระจายการจัดเก็บในหลายโหนดของบล็อกเชน (distributed ledgers) ทั้งนี้เพื่อเป็นข้อมูลหลักฐานที่ยืนยันความถูกต้องตรงกันในหลายโหนดนั้น ซึ่งส่งผลให้เกิดการยืนยันไม่ให้เกิดการแก้ไขบิดพลิ้วโดยมิชอบ

5) การเตรียมบุคลากรของหน่วยงานภาครัฐให้มีความรู้ความเข้าใจ และมีทักษะในการพัฒนาระบบบล็อก เป็นความท้าทายที่สำคัญยิ่ง ทั้งในด้านการพัฒนา บำรุงรักษาและต่อยอดขยายผลของระบบในอนาคต

6) เนื่องจากข้อมูลในกระบวนการยุติธรรมเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว (sensitive personal data)จึงเสนอให้ใช้ระบบบล็อกเชนแบบ Private/Consortium Blockchain เพื่ออนุญาตให้เฉพาะผู้ดูแลระบบหรือผู้ใช้ที่ได้รับอนุญาตกลุ่มหนึ่งเท่านั้นที่จะเข้าถึงข้อมูลเหล่านั้นได้ภายใต้เงื่อนไขหรือสิทธิ์ในการเข้าถึงข้อมูลด้วยบทบาทที่กำหนดไว้ตามกฎหมาย

7) แพลตฟอร์มที่เสนอให้เลือกใช้สำหรับการพัฒนาระบบต้นแบบบล็อกเชน คือ Hyperledger Fabric ซึ่งเป็นซอฟต์แวร์แบบเปิดเผยรหัสโปรแกรม (opensource) การเลือกใช้ซอฟต์แวร์แบบเปิดเผยรหัสโปรแกรมนี้ช่วยทำให้ประหยัดค่าใช้จ่ายในการพัฒนาระบบ อีกทั้งมีกลุ่มผู้ใช้งานและผู้ที่มีความรู้และทักษะในการพัฒนาของแพลตฟอร์มบล็อกเชนนี้ค่อนข้างกว้างขวางในประเทศไทย

8) เนื่องจากหลักฐานพยาน เช่น ภาพถ่ายและวิดีโอเป็นข้อมูลขนาดใหญ่ ดังนั้นโครงการวิจัยนี้เสนอให้ใช้วิธีการออกแบบการจัดเก็บข้อมูลในบล็อกเชนเฉพาะส่วนที่เป็น Hashing value นั้น คือ ค่าเฉพาะที่ได้จากการคำนวณเนื้อหาของข้อมูลด้วยฟังก์ชันทางคณิตศาสตร์ เป็นเสมือนลายนิ้วมือของข้อมูล ใช้ยืนยันความถูกต้องครบถ้วนของข้อมูล โดยค่านี้มักเป็นเลขฐาน 16 ความยาวแน่นอนของไฟล์หลักฐานพยานขึ้นอยู่กับฟังก์ชันที่ใช้ ที่นิยมได้แก่ MD5 ซึ่งมีขนาด 16 ไบต์ (128 บิต) ทั้งนี้ เพื่อให้เกิดการประหยัดพื้นที่จัดเก็บข้อมูลและเพิ่มประสิทธิภาพความเร็วในการประมวลผลของบล็อกเชน ทั้งนี้หน่วยงานที่ต่อเชื่อมเป็น Blockchain Peer จะต้องมีระบบการจัดการเอกสาร และข้อมูลอิเล็กทรอนิกส์กลางขององค์กรด้วย (ระบบ Document Management System: DMS)

9) แบบจำลองของการพัฒนาระบบบล็อกเชนสำหรับกระบวนการยุติธรรมในอนาคตจะเป็นการพัฒนาแบบต่อยอดจากระบบสารสนเทศที่มีอยู่แล้วในแต่ละหน่วยงาน แต่ให้มีการเชื่อมโยงกันในลักษณะเครือข่าย Distributed ledgers (blockchain) Network เช่น เชื่อมโยงระบบ CRIMES ของสำนักงานตำรวจแห่งชาติ ระบบสารบบคดีอิเล็กทรอนิกส์ของสำนักงานอัยการสูงสุด และระบบ Smart Court สำนักงานของศาลยุติธรรม

การพัฒนาในอนาคตควรมีการออกแบบกระบวนการ (To - Be Process) และจัดทำรูปแบบข้อมูลที่จะเชื่อมโยงและแลกเปลี่ยน (To-Be Data Architecture) ตามสถานการณ์การปฏิบัติงาน

ยุติธรรมด้านต่าง ๆ ในรายละเอียด ก่อนที่จะมีการพัฒนาระบบแบบเต็มรูป รวมทั้งควรมีการประเมินงบและจัดทำแผนการพัฒนาที่ชัดเจนในลำดับต่อไป

บรรณานุกรม

ชัยพร ทบแป, ประสงค์ ประณีตพลกรัง และนิเวศ จิระวิชิตชัย. (2563). โมเดลสมการโครงสร้างของปัจจัยที่ส่งผลต่อการจัดทำกรอบสถาปัตยกรรมการสับเปลี่ยนเอกสารธุรกรรมอิเล็กทรอนิกส์ด้วยเทคโนโลยีบล็อกเชน. *วารสารศรีปทุมปริทัศน์ ฉบับวิทยาศาสตร์และเทคโนโลยี, 12,* 79-92.

ประดิษฐ์ แป้นทอง. (2558). ปัญหาและแนวทางในการพัฒนากระบวนการยุติธรรมของประเทศไทย, *วารสารกฎหมาย. 8*(16), 31-44.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2560). *บทนำเกี่ยวกับเทคโนโลยีความปลอดภัยของข้อมูล.* ค้นเมื่อ 15 พฤษภาคม 2563, จาก https://www.nrca.go.th/content/02-1.html

สำนักงานพัฒนารัฐบาลดิจิทัล. (2562). *การใช้เทคโนโลยีบล็อกเชนสำหรับภาครัฐ.* ค้นเมื่อ 15 พฤษภาคม 2563, จาก https://www.dga.or.th/upload/download/file_ff487bacfb3198a615ca75112b8d156c.pdf

สำนักงานสถิติแห่งชาติ. (2563). *แผนแม่บทระบบสถิติของประเทศ, รายงานการติดตามระดับพื้นที่ ประจำปีงบประมาณ พ.ศ. 2563 ด้านสังคม สาขายุติธรรม ความมั่นคง การเมืองและการปกครอง.* ค้นเมื่อ 15 พฤษภาคม 2563, จาก https://oslist.smpnso.go.th/report/stat/mission/detail?dmt=1&Year=2563&SubjectId=12

หนังสือต่างประเทศ

Chaisuriya, S., Keretho, S., Sanguanpong, S., & Praneetpolgrang, P. (2018). *A Security Architecture Framework for CriticalInfrastructure with Ring-based Nested Network Zones.* 2018 10th International Conference on Knowledge and Smart Technology (KST). 248-253.

Chaisuriya, S., Keretho, S., Sanguanpong, S., & Thoppae, C. (2021). Ring-Based cybersecurity architecture for critical infrastructure. *Turkish Journal of Computer and Mathematics Mathematics Education, 12*(6), 2826-2840.

Comrey, A. L., & Lee, H. B. (2013). *A first course in factor analysis* (2nd ed.). NY: Psychology Press.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). LA: Sage Publications.

Department of Defense Standard. (1985). *Department of defense trusted computer system evaluation criteria. Fort Meade: National Computer Security Center.* Retrieved May 25, 2020 from https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs- papers/dod85.pdf

e-Estonia. (2020). *e-law.* Retrieved May 25, 2020, from https://eestonia.com/solutions/security-and-safety/e-law

Guardtime. (2020). *KSI blockchain in Estonia.* Retrieved May 25, 2020, from https://e-estonia.com/wp-content/uploads/2020mar-faq-ksi-blockchain-1-1.pdf

ISECT. (2012). *Guidelines for the design and implementation of network security.* Retrieved May 15, 2020, from https://www.iso.org/standard/51581.html?browse=tc

Supreme People's Court of the People's Republic of China. (2019). *Chinese courts and internet judiciary.* Retrieved May 25, 2020, from http://english.court.gov.cn/2019-12/18/content_37529518.htm

Thoppae, C., & Jirawichitchai, N. (2020). A Blockchain Secured Electronic Transaction Document Interchange Architecture (DIA) : A Public Sector Analysis from Thailand. *International Journal of Innovation, Creativity and Change. 14*(12), 1153-1172.

Thoppae, C., & Praneetpolgrang, P. (2021). An analysis of a blockchain-enabled e-government Document Interchange Architecture (DIA) in Thailand. *Technology Education Management Informatics, 1*0(3), 1220-1227.

Thoppae, C., Praneetpolgrang, P., & Jirawichitchai, N. (2021). Development of Efficient and Secured Electronic Transaction Document Interchange Architecture Framework among Public Sector with Blockchain Technology. *Information Technology Journal, 17*(1), 66-75.