การพัฒนา BLOCKCHAIN นวัตกรรมแห่งอนาคต

สำหรับผู้เริ่มต้นที่จะสร้างถนนแห่งความสำเร็จ
ทางด้านธุรกรรมการเงินในยุค DISRUPTION

ใหม่ล่าสุด

รองศาสตราจารย์ ดร. พรรณี สวนเพลง
พัฒนพงษ์ โพธิปัสสา

ซีเอ็ด

การพัฒนา Blockchain นวัตกรรมแห่งอนาคต

โดย รศ.ดร. พรรณี สวนเพลง และพัฒนพงษ์ โพธิปัสสา

ข้อมูลทางบรรณานุกรมของหอสมุดแห่งชาติ

พัฒนพงษ์ โพธิปัสสา.

การพัฒนา Blockchain นวัตกรรมแห่งอนาคต. -- กรุงเทพฯ : ซีเอ็ดยูเคชั่น, 2566.

408 หน้า.

1. บิทคอยน์. 2. การพาณิชย์อิเล็กทรอนิกส์.

I. พรรณี สวนเพลง, ผู้แต่งร่วม. II. ชื่อเรื่อง.

332.4

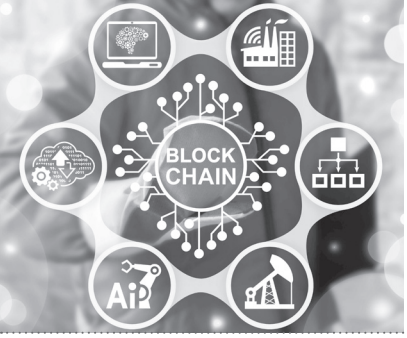
Barcode (e-book) : 9786160850471

ผลิตและจัดจำหน่ายโดย

บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน)
SE-EDUCATION PUBLIC COMPANY LIMITED

เลขที่ 1858/87–90 ถนนเทพรัตน แขวงบางนาใต้ เขตบางนา กรุงเทพฯ 10260
โทรศัพท์ 0–2826–8000

หากมีคำแนะนำหรือติชม สามารถติดต่อได้ที่ comment@se-ed.com



คำนำ

หนังสือ *การพัฒนา Blockchain นวัตกรรมแห่งอนาคต* เป็นหนังสือเล่มแรกที่ตีพิมพ์เป็นภาษาไทยโดยมุ่งหวังให้เป็นการ “บุกเบิก” องค์ความรู้ทางด้านการพัฒนาเทคโนโลยีบล็อกเชนให้เกิดขึ้นอย่างเป็นรูปธรรมในประเทศไทย เนื่องจากปัจจุบันการเปลี่ยนถ่ายเข้าสู่ยุคดิจิทัลได้ส่งผลให้การทำธุรกรรมต่าง ๆ ต้องการความปลอดภัย ความเป็นส่วนตัว การประมวลผลแบบกระจาย แต่ต้องการความเชื่อมั่นในข้อมูลและกระบวนการที่เกี่ยวข้องมากยิ่งขึ้น ทว่าหากขาดแหล่งข้อมูล หรือเอกสารอ่านประกอบการพัฒนาให้กับผู้ที่สนใจ

หนังสือเล่มนี้เขียนจากประสบการณ์ในการทำงานวิชาการและงานวิจัยทางด้านเทคโนโลยีสารสนเทศ รวมถึงประสบการณ์การทำงานด้านระบบคอมพิวเตอร์ตั้งแต่เริ่มมีเว็บเซอร์วิซ (Web Service) เข้ามาในประเทศไทยเพื่อทำให้เกิดการแลกเปลี่ยนและใช้งานข้อมูลร่วมกันระหว่างคอมพิวเตอร์ที่มีสถาปัตยกรรมที่แตกต่างกัน จนกระทั่งในปัจจุบันที่ระบบการประมวลผลของคอมพิวเตอร์ทั่วโลกได้เปลี่ยนจากการประมวลผลแบบรวมศูนย์กลางมาเป็นระบบประมวลผลเชิงกระจาย ซึ่งทำให้การเรียนรู้ การพัฒนาระบบและแอปพลิเคชันที่เกี่ยวข้องเปลี่ยนแปลงไปจากเดิมโดยสิ้นเชิง และนำมาสู่การใช้เทคโนโลยีบล็อกเชนในปัจจุบัน

นอกจากนี้หนังสือเล่มนี้เขียนจากประสบการณ์ทำงานวิจัยที่เกี่ยวข้องกับการพัฒนาระบบบล็อกเชนเพื่อนำมาประยุกต์ใช้สำหรับธุรกิจและการท่องเที่ยว รวมถึงงานบริการวิชาการที่มีเนื้อหาสาระทางด้านนวัตกรรมการพัฒนาบล็อกเชน และได้ถูกนำมายกตัวอย่างเพื่อเป็นกรณีศึกษาและเป็นแนวทางในการพัฒนาต่อยอดองค์ความรู้ในหนังสือเล่มนี้ อีกทั้งยังมีการรวบรวมองค์ความรู้จากหนังสือ บทความวิจัย บทความวิชาการ เอกสารจากต่างประเทศ เพื่อให้ได้ข้อมูลและองค์ความรู้ที่ทันสมัย อีกทั้งยังได้จัดทำรูปประกอบขึ้นเองในรูปแบบของอินโฟกราฟิก (Infographic) โดยหนังสือเล่มนี้มีขอบเขตของเนื้อหาประกอบไปด้วย

Part I ความรู้พื้นฐานเกี่ยวกับเทคโนโลยีบล็อกเชน (Introduction to Blockchain) ซึ่งครอบคลุมเนื้อหาบทที่ 1–5 ที่เป็นความรู้พื้นฐานทางทฤษฎีเกี่ยวกับบล็อกเชน การทำธุรกรรม ความปลอดภัยของบล็อกเชน อีเทอเรียมบล็อกเชน (Ethereum Blockchain) และดีแอป (DApp)

Part II การพัฒนาบล็อกเชนด้วยอีเทอเรียมรีมิกซ์ (Blockchain Development by Ethereum Remix) ครอบคลุมเนื้อหาบทที่ 6–13 ที่นำเสนอแนวทางการพัฒนาระบบบล็อกเชนด้วยอีเทอเรียมรีมิกซ์ ได้แก่ สภาพแวดล้อมการพัฒนาบล็อกเชน การใช้งานโปรแกรม อีเทอเรียมรีมิกซ์ การเขียนโปรแกรมด้วยภาษาโซลิดิตี (Solidity) และการสร้างสัญญาอัจฉริยะหรือสมาร์ตคอนแทรกต์ (Smart Contract)

Part III ตัวอย่างและกรณีศึกษาการพัฒนาบล็อกเชน (Blockchain Development Case Study) ครอบคลุมเนื้อหาบทที่ 14–15 เป็นการนำเสนอตัวอย่างการพัฒนาระบบบล็อกเชน และนำเสนอตัวอย่างกรณีศึกษาที่ประยุกต์ใช้ระบบบล็อกเชนในอุตสาหกรรมต่าง ๆ นอกจากนี้ยังใช้เป็นเครื่องมือและช่องทางของการพัฒนาบล็อกเชนเพื่อการศึกษาค้นคว้าและพัฒนาต่อยอดนวัตกรรมขั้นสูงต่อไป

ผู้เขียนมีความตั้งใจให้หนังสือเล่มนี้เป็นประโยชน์ในวงกว้างสองแนวทาง โดยแนวทางแรกใช้เป็นคู่มืออ้างอิงสำหรับนักเรียน นิสิต นักศึกษาที่สนใจและเริ่มต้นในการพัฒนาระบบบล็อกเชน และแนวทางที่สองสำหรับผู้สนใจทั่วไปใช้หนังสือเล่มนี้ เพื่อเริ่มต้นพัฒนาระบบบล็อกเชนที่สามารถนำไปประยุกต์ใช้ในองค์กร หน่วยงาน องค์กรทั้งภาครัฐและเอกชน และเกิดแรงบันดาลใจในการเตรียมความพร้อมเพื่อถ่ายโอนข้อมูลและรูปแบบการทำงานเข้าสู่ยุคของเทคโนโลยีบล็อกเชนเพื่อให้ประเทศไทยสามารถดำเนินกิจกรรมทั้งภาครัฐและภาคธุรกิจร่วมกับนานาประเทศได้อย่างมีประสิทธิภาพ เกิดความโปร่งใส และมีความน่าเชื่อถือในระดับสูง

กว่าหนังสือเล่มนี้จะเขียนสำเร็จและตีพิมพ์เป็นรูปเล่มได้ต้องอาศัยปัจจัยหลายประการประกอบกัน ที่สำคัญที่สุดผู้เขียนขอกราบขอบพระคุณหน่วยงานที่มอบทุนสนับสนุนการวิจัยที่ได้ทำงานวิจัยเกี่ยวกับการพัฒนาระบบบล็อกเชนที่เป็นองค์ความรู้นำมาใช้ถ่ายทอดในหนังสือเล่มนี้ รวมถึงท่านผู้ทรงคุณวุฒิ (Peer Review) ที่ช่วยตรวจและประเมินเนื้อหาในหนังสือเพื่อให้ได้คุณภาพตามมาตรฐานทางวิชาการ ทีมงานที่ช่วยในการพิมพ์งาน งานตรวจทานข้อมูล งานศิลป์ งานพิสูจน์อักษร งานจัดรูปแบบ การเข้าเล่ม และการประสานกับทุกฝ่ายจนสำเร็จ ทำให้หนังสือเล่มนี้มีความสมบูรณ์ ถูกต้อง ทันสมัย ท้ายที่สุดนี้หากหนังสือเล่มนี้มีข้อผิดพลาดผู้เขียนขอน้อมรับไว้ และหากท่านผู้อ่านมีข้อเสนอแนะที่เป็นประโยชน์ต่อการปรับปรุงหนังสือเล่มนี้ให้ดียิ่งขึ้น ผู้เขียนขอกราบขอบพระคุณและขอน้อมรับไว้แก้ไขในโอกาสต่อไป

รองศาสตราจารย์ ดร. พรรณี สวนเพลง
อาจารย์พัฒนพงษ์ โพธิปัสสา

คำชี้แจงในการใช้หนังสือ

หนังสือ *การพัฒนา Blockchain นวัตกรรมแห่งอนาคต* ประกอบด้วยเนื้อหาแบ่งออกเป็น 3 ส่วนดังนี้

Part I ความรู้พื้นฐานเกี่ยวกับเทคโนโลยีบล็อกเชน (Introduction to Blockchain)

มีเนื้อหาครอบคลุมความรู้พื้นฐานในเชิงทฤษฎีเกี่ยวกับบล็อกเชน ซึ่งประกอบด้วย

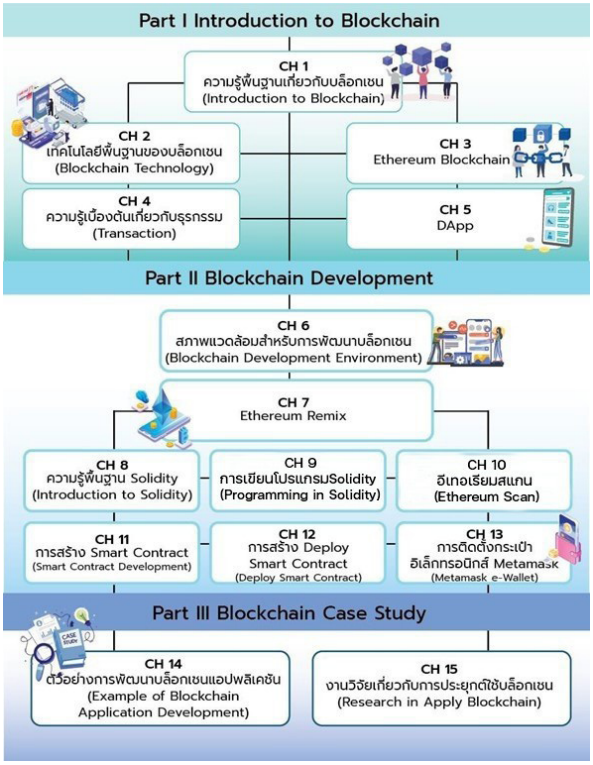
บทที่ 1 ความรู้พื้นฐานของบล็อกเชน (Introduction to Blockchain) มีเนื้อหาครอบคลุมเกี่ยวกับความหมายและความรู้เบื้องต้นเกี่ยวกับบล็อกเชน การทำงานของบล็อกเชน การทำธุรกรรมในบล็อกเชน การจำแนกประเภทของบล็อกเชน ประโยชน์ของเทคโนโลยีบล็อกเชน แนวทางการประยุกต์ ใช้เทคโนโลยีบล็อกเชน ประเด็นที่ควรให้ความสำคัญด้านเทคโนโลยีที่เกี่ยวข้องกับเทคโนโลยีบล็อกเชน และกรณีศึกษาและงานวิจัยเกี่ยวกับเทคโนโลยีบล็อกเชน

บทที่ 2 เทคโนโลยีพื้นฐานของบล็อกเชน (Blockchain Technology) มีเนื้อหาครอบคลุมเกี่ยวกับสถาปัตยกรรมของบล็อกเชน ทฤษฎีพื้นฐานของบล็อกเชน ความปลอดภัยของบล็อกเชนฟังก์ชันแฮช (Hash Function), อี–สแตมป์ (E–stamp), เครือข่าย P2P (Peer–to–Peer Network) และกรณีศึกษาและงานวิจัยเกี่ยวกับเทคโนโลยีพื้นฐานบล็อกเชน

บทที่ 3 อีเทอเรียมบล็อกเชน (Ethereum Blockchain) มีเนื้อหาครอบคลุมเกี่ยวกับสถาปัตยกรรมของบล็อกเชน ทฤษฎีพื้นฐานของบล็อกเชน และเทคโนโลยีที่เกี่ยวข้องกับความปลอดภัยของบล็อกเชน เนื้อหาในบทนี้จะอธิบายเนื้อหาเกี่ยวกับอีเทอเรียมบล็อกเชน โดยมีเนื้อหาครอบคลุมเกี่ยวกับอีเทอเรียมแพลตฟอร์ม (Ethereum Platform) ประวัติของอีเทอเรียม ทัวริงสมบูรณ์ (Turing Complete), อีเทอร์ (Ether) สถาปัตยกรรมของอีเทอเรียม (Ethereum Architecture) ธุรกรรมในอีเทอเรียม (Ethereum Transaction), โหนด (Nodes) EVM, Mining Nodes และบัญชี (Account)

บทที่ 4 ความรู้เบื้องต้นเกี่ยวกับธุรกรรม (Transaction) มีเนื้อหาครอบคลุมเกี่ยวกับความหมายและความรู้เบื้องต้นเกี่ยวกับธุรกรรม ประเภทของธุรกรรม วงจรชีวิตของการทำธุรกรรม ค่าแก๊ส (Gas) การตั้งค่าและคำนวณค่าน้ำมัน การเปลี่ยนแปลงสถานะของข้อมูลที่เกี่ยวข้องกับการทำธุรกรรม และกรณีศึกษาและงานวิจัยเกี่ยวกับธุรกรรมในบล็อกเชน

บทที่ 5 ดีแอป (DApp) มีเนื้อหาครอบคลุมเกี่ยวกับนิยามของดีแอป สถาปัตยกรรมของอีเทอเรียมดีแอป (Ethereum DApp) ข้อดีข้อเสียของการพัฒนาดีแอป เครื่องมือสำหรับพัฒนาดีแอป และดีแอปเบราว์เซอร์ (DApp Browser) การพัฒนาสัญญาอัจฉริยะ (Smart Contract Development) ความแตกต่างระหว่าง Centralized Client Server และ Decentralized Client DApp และกรณีศึกษาและงานวิจัยที่เกี่ยวข้องกับดีแอป



Part II การพัฒนาบล็อกเชน (Blockchain Development)

นำเสนอแนวทางการพัฒนาระบบบล็อกเชนด้วยอีเทอเรียมรีมิกซ์ ซึ่งประกอบด้วย

บทที่ 6 สภาพแวดล้อมสำหรับการพัฒนาโปรแกรม (Blockchain Environment) มีเนื้อหาครอบคลุมความรู้พื้นฐานเกี่ยวกับสถาปัตยกรรมของแอปพลิเคชันเชิงกระจาย (DApp

Architecture) สภาพแวดล้อมในการประมวลผลสัญญาอัจฉริยะ สภาพแวดล้อมการทำงานที่ใช้เมตามาสก์ (MetaMask) เพื่อการเชื่อมต่อกับเครือข่ายอีเทอเรียม (Ethereum Network) กรอบการทำงานที่จำเป็นต่อการพัฒนาอีเทอเรียมดีแอป (Ethereum DApp) อีเทอเรียมสแต็ก (Ethereum Stack) อีเทอเรียมไคลเอนต์ (Ethereum Client) เครือข่ายอีเทอเรียม การพัฒนาเครือข่าย การพัฒนาสภาพแวดล้อม (Integrated Development Environment) และกรณีศึกษาและงานวิจัยที่เกี่ยวกับสภาพแวดล้อมของการพัฒนาโปรแกรม (Blockchain Development)

บทที่ 7 อีเทอเรียมรีมิกซ์ (Ethereum Remix) มีเนื้อหาครอบคลุมเกี่ยวกับความรู้พื้นฐานโปรแกรมอีเทอเรียมรีมิกซ์ ส่วนประกอบในอีเทอเรียมรีมิกซ์ เครื่องมือในแถบ Icon Panel ชุดคำสั่งภายใต้ File Explorers ชุดคำสั่งภายใต้คอมไพเลอร์ของโซลิดิตี (Solidity Compilers) ชุดคำสั่งภายใต้การปรับใช้และทำธุรกรรม (Deploy & Run Transactions) ชุดคำสั่งภายใต้ตัวจัดการปลั๊กอิน (Plugin Manager) ชุดคำสั่งภายใต้การเซตติง (Settings) และกรณีศึกษาและงานวิจัยที่เกี่ยวข้องกับโปรแกรมอีเทอเรียมรีมิกซ์

บทที่ 8 ความรู้พื้นฐานโซลิดิตี (Introduction to Solidity) มีเนื้อหาครอบคลุมเกี่ยวกับความรู้พื้นฐานภาษาโซลิดิตี (Solidity Language) ซึ่งเป็นโปรแกรมสำหรับการพัฒนาระบบบล็อกเชน มีรายละเอียดครอบคลุมเกี่ยวกับแนวคิดของการเขียนโปรแกรมโซลิดิตี โครงสร้างของโซลิดิตี การใช้งานโซลิดิตี หน่วยความจำเปรียบเทียบกับการจัดเก็บ (Memory vs Storage) Basic Types ในโซลิดิตี ประเภทของตัวแปร (Types of Variables) โครงสร้างข้อมูล (Data Structures) การเขียนโปรแกรมในโซลิดิตี และกรณีศึกษาและงานวิจัยที่เกี่ยวข้องกับการใช้งานโซลิดิตี

บทที่ 9 การเขียนโปรแกรมโซลิดิตี (Programming in Solidity) มีเนื้อหาครอบคลุมเกี่ยวกับประเภทของตัวแปรในโซลิดิตี ตัวดำเนินการในภาษาโซลิดิตี การวนลูปในภาษาโซลิดิตี การตัดสินใจในโซลิดิตี ฟังก์ชันใน Solidity Function Modifiers View Function และกรณีศึกษาและงานวิจัยที่เกี่ยวข้องกับการเขียนโปรแกรมด้วยภาษาโซลิดิตี

บทที่ 10 อีเทอเรียมสแกน (Ethereum Scan) มีเนื้อหาครอบคลุมความรู้พื้นฐานเกี่ยวกับอีเทอเรียมสแกน การตรวจสอบกระเป๋าเงิน ETH และโทเค็นบนอีเทอเรียมสแกน การตรวจสอบรหัสพันธุกรรม Txn Hash การตรวจสอบสมาร์ตคอนแทรกต์ การตรวจสอบยอดโทเค็น ERC20 ในที่อยู่ ETH การติดตามธุรกรรมบน DEX การใช้อีเทอร์สแกน การใช้อีเทอร์สแกน เพื่อตรวจสอบค่าแก๊ส (Gas) การค้นหาแอร์ดร็อป (Air Drop) บนอีเทอร์สแกน และกรณีศึกษาและงานวิจัยที่เกี่ยวข้องกับอีเทอเรียมสแกน

บทที่ 11 การสร้างสมาร์ตคอนแทรกต์ (Smart Contract) มีเนื้อหาครอบคลุมเกี่ยวกับการสลับไปที่ Test Network การรับเหรียญ ETH ฟรีเพื่อใช้ในการทดสอบ การสร้างสมาร์ตคอนแทรกต์แรก ภาพรวมในการปรับใช้สมาร์ตคอนแทรกต์ (Deploy Smart Contract) และแก๊สบนอีเทอเรียม ตัวอย่างโค้ดสำหรับเรียนรู้การปรับใช้สมาร์ตคอนแทรกต์ และกรณีศึกษาและงานวิจัยที่เกี่ยวข้องกับการสร้างสมาร์ตคอนแทรกต์

บทที่ 12 การปรับใช้สมาร์ตคอนแทรกต์ (Deploy Smart Contract) มีเนื้อหาครอบคลุมเกี่ยวกับ Deploy Smart Contract และการกำหนดค่าแก๊ส ซึ่งกระบวนการ Deployment Smart Contract นั้นทำให้เรียกใช้ดีแอป (DApp) ที่นักพัฒนาสร้างขึ้นและทำงานได้บนเครือข่ายบล็อกเชน ส่วนการกำหนดค่าแก๊สหรือค่าธรรมเนียมในการทำธุรกรรมนั้นเป็นสิ่งจำเป็นในการทำธุรกรรมบนเครือข่ายอีเทอเรียมซึ่งนักพัฒนาจะต้องกำหนดให้อยู่ในระดับที่เหมาะสม

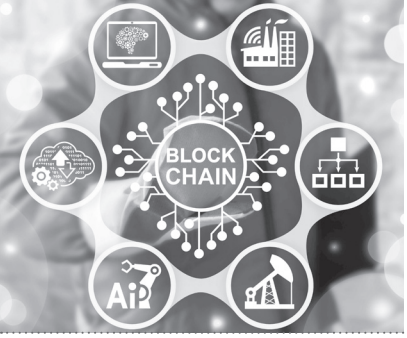
บทที่ 13 การติดตั้งกระเป๋าอิเล็กทรอนิกส์เมตามาสก์ (MetaMask) มีเนื้อหาครอบคลุมความรู้พื้นฐานเกี่ยวกับเมตามาสก์ การติดตั้งเมตามาสก์บนระบบปฏิบัติการวินโดวส์ และกรณีศึกษาและงานวิจัยที่เกี่ยวข้องกับการติดตั้งกระเป๋าอิเล็กทรอนิกส์เมตามาสก์

Part III กรณีศึกษาการพัฒนาบล็อกเชน (Blockchain Case Study)

มีเนื้อหาครอบคลุมเกี่ยวกับตัวอย่างการพัฒนาระบบบล็อกเชน และนำเสนอตัวอย่างกรณีศึกษาที่ประยุกต์ใช้ระบบบล็อกเชนในอุตสาหกรรมต่าง ๆ นอกจากนี้ยังใช้เป็นเครื่องมือและช่องทางของการพัฒนาบล็อกเชนเพื่อการศึกษาค้นคว้าและพัฒนาต่อยอดนวัตกรรมขั้นสูงต่อไป

บทที่ 14 ตัวอย่างการพัฒนาบล็อกเชนแอปพลิเคชัน (Example of Blockchain Application Development) มีเนื้อหาครอบคลุมเกี่ยวกับการฝาก (Deposit) การออกเสียง (Vote) โปรแกรม SimpleBank การ Shared Wallet การจัดเก็บจำนวนเต็มอย่างง่าย (Simple Storage) และกรณีศึกษาและงานวิจัยที่เกี่ยวข้องกับการพัฒนาบล็อกเชนแอปพลิเคชัน

บทที่ 15 งานวิจัยเกี่ยวกับการประยุกต์ใช้บล็อกเชน (Case Study of Apply Blockchian) มีเนื้อหาครอบคลุมเกี่ยวกับ การใช้งานบล็อกเชนทางการแพทย์ การประยุกต์ใช้บล็อกเชนกับการท่องเที่ยว และการประยุกต์ใช้บล็อกเชนกับการเกษตร



สารบัญ

บทที่ 1
ความรู้พื้นฐานของบล็อกเชน
(Introduction to Blockchain Technology)

ด้วยความก้าวหน้าของเทคโนโลยีในยุคดิสรัปชัน (Disruption) ทำให้เกิดการปฏิวัติวิถีชีวิตของมนุษย์ด้วยเทคโนโลยีสารสนเทศ ก่อให้เกิดการพัฒนานวัตกรรมเพื่อนำมาประยุกต์ใช้ให้เท่าทันการเปลี่ยนแปลง (Transformation) โดยเฉพาะอย่างยิ่งได้มีการนำบล็อกเชน (Blockchain) ซึ่งเป็นเทคโนโลยีที่มีความทันสมัยมาประยุกต์ใช้ในหลากหลายอุตสาหกรรม และมีแนวโน้มการเติบโตแบบก้าวกระโดดในทุกมุมโลก บล็อกเชนเป็นเทคโนโลยีที่สำคัญในการเปลี่ยนแปลงรูปแบบของการทำธุรกรรมของโลกอนาคต

เนื้อหาประจำบท

1. ความรู้เบื้องต้นเกี่ยวกับบล็อกเชน
2. สถาปัตยกรรมของบล็อกเชน
3. การทำงานและการทำธุรกรรมในบล็อกเชน
4. ประเภทของบล็อกเชน
5. ประโยชน์ของเทคโนโลยีบล็อกเชน
6. แนวทางการประยุกต์ใช้เทคโนโลยีบล็อกเชน
7. กรณีศึกษาและงานวิจัยเกี่ยวกับเทคโนโลยีบล็อกเชน

วัตถุประสงค์

1. อธิบายความหมายและความรู้เบื้องต้นเกี่ยวกับบล็อกเชนได้
2. เข้าใจถึงโครงสร้างและสถาปัตยกรรมของบล็อกเชนได้
3. เข้าใจและอธิบายการทำงานและการทำธุรกรรมในบล็อกเชนได้
4. อธิบายประเภทของบล็อกเชนได้
5. อธิบายประโยชน์ของเทคโนโลยีบล็อกเชนได้
6. อธิบายแนวทางการประยุกต์ ใช้เทคโนโลยีบล็อกเชนในอุตสาหกรรมต่าง ๆ ได้
7. ประยุกต์ความรู้จากกรณีศึกษาและงานวิจัยเกี่ยวกับเทคโนโลยีบล็อกเชนได้

1.1 ความรู้เบื้องต้นเกี่ยวกับบล็อกเชน

บล็อกเชน (Blockchain) เป็นนวัตกรรมทางด้านเทคโนโลยีสารสนเทศในยุคปัจจุบัน ที่เริ่มมีการนำมาประยุกต์ใช้กันอย่างแพร่หลายในหลากหลายมิติและอุตสาหกรรม ดังนั้นจึงความจำเป็นที่จะต้องทราบถึงความรู้พื้นฐานเกี่ยวกับบล็อกเชน ซึ่งในหัวข้อนี้ประกอบด้วย ความหมายของบล็อกเชน วิวัฒนาการของบล็อกเชน คุณลักษณะของบล็อกเชน และส่วนประกอบของเครือข่ายบล็อกเชน มีรายละเอียดดังนี้

1.1.1 ความหมายของบล็อกเชน

มีนักวิชาการได้นิยามความหมายของบล็อกเชนไว้ต่าง ๆ ดังนี้

รูปที่ 1.1 บล็อกเชน

นิยามของบล็อกเชน (Blockchain Definition) หมายถึงเทคโนโลยีที่มีความปลอดภัยในการจัดเก็บข้อมูล และสามารถใช้ข้อมูลร่วมกันได้ของผู้ใช้งานบนระบบ หากจะมีการบันทึกข้อมูลหรือการปรับปรุงข้อมูลจะต้องได้รับการอนุญาตจากสมาชิกในเครือข่ายก่อนจึงจะปรับปรุงข้อมูลได้ (Bashir, 2020)

นิยามของบล็อกเชนทางด้านเทคนิค (Blockchain Technical Definition) หมายถึง การจัดเก็บข้อมูลลงในบล็อก (Block) และถูกเชื่อมต่อกันด้วยโซ่ (Chain) (ดังแสดงในรูปที่ 1.1) ที่สร้างขึ้นเพื่อกระจายข้อมูลเก็บไว้ในชิ้นส่วนของโซ่ที่ต่อกัน โดยข้อมูลเหล่านั้นไม่สามารถเปลี่ยนแปลงได้ จากการใช้เทคโนโลยีการจัดเก็บข้อมูลแบบแชร์ฐานข้อมูล (Share Databased) หรือที่เรียกว่า Distributed Ledger Technology (DLT) ซึ่งเป็นรูปแบบของการจัดเก็บข้อมูลที่มีความปลอดภัย โดยใช้หลักการคริปโทกราฟี (Cryptography)[1] ที่มีความสามารถในการบริหารจัดการข้อมูล ระบบเครือข่าย และการทำงานสนับสนุนร่วมกันเพื่อตรวจสอบ ประมวลผล และบันทึกข้อมูลระหว่างผู้ใช้งานระบบเครือข่ายและความสามารถ

[1] หมายเหตุ : Cryptography ในหนังสือเล่มนี้จะใช้คำว่า คริปโทกราฟี

ของการกระจายของคอมพิวเตอร์และการประมวลผล (Distributed Computing) เพื่อสร้างความน่าเชื่อถือของข้อมูล (Bashir, 2020; Yermack, 2017; Xu et al., 2019)

นอกจากนี้บล็อกเชนคือ ชุดของข้อมูลที่จัดเก็บทางอิเล็กทรอนิกส์ในระบบคอมพิวเตอร์ ข้อมูลหรือข้อมูลในฐานข้อมูลมักมีโครงสร้างในรูปแบบตารางเพื่อให้สามารถค้นหาและกรองข้อมูลเฉพาะได้ง่ายขึ้น โดยใช้สเปรดชีต (Spreadsheet) เพื่อจัดเก็บข้อมูลมากกว่าฐานข้อมูลขนาดใหญ่ (Big Data) ซึ่งทำได้โดยอาศัยข้อมูลบนเซิร์ฟเวอร์ (Server) (Investopedia, 2021)

ทั้งนี้การทำธุรกรรมบนบล็อกเชนจะต้องมีการตรวจสอบ หรือการทำ "ฉันทามติ" (Consensus)[2] จากทั้งเครือข่ายเสียก่อน จึงจะสามารถบันทึกข้อมูลลงในบล็อกได้ ทำให้เทคโนโลยีบล็อกเชนไม่จำเป็นต้องมีตัวกลางในการทำหน้าที่จัดเก็บข้อมูลรายการทำธุรกรรม แต่ข้อมูลทั้งหมดจะถูกจัดเก็บภายในโครงสร้างของเทคโนโลยีบล็อกเชน และถูกกระจาย (Distributed) ไปยังเครื่องของสมาชิกทุกคนในเครือข่าย และหากมีคนพยายามสร้างรายการทำธุรกรรมปลอมขึ้นมา จะทำให้ข้อมูลนั้นไม่ตรงกับที่อยู่ในเครื่องของสมาชิกคนอื่น ๆ ในเครือข่าย ทำให้ระบบไม่อนุมัติในการสร้างรายการดังกล่าวได้ ทั้งนี้ข้อมูลที่ถูกบันทึกเข้าสู่ระบบบล็อกเชนไปแล้วจะไม่สามารถแก้ไขหรือเปลี่ยนแปลงได้ ด้วยเหตุดังกล่าวจึงทำให้เทคโนโลยีบล็อกเชนได้รับการยอมรับว่าเป็นเทคโนโลยีที่มีความปลอดภัย น่าเชื่อถือ มีความโปร่งใส และการกระจายอำนาจ (สำนักงานพัฒนารัฐบาลดิจิทัล, 2564)

อย่างไรก็ตาม เพื่อให้เข้าใจบล็อกเชนมากขึ้น ลองพิจารณาตัวอย่าง การมองหาตัวเลือกในการส่งเงินไปให้เพื่อนที่อาศัยอยู่ในต่างประเทศ ซึ่งตัวเลือกทั่วไปที่ผู้ใช้สามารถใช้ได้ตามปกติอาจเป็นธนาคารหรือผ่านแอปพลิเคชันการโอนเงิน เช่น เพย์พาล (PayPal) ตัวเลือกนี้เกี่ยวข้องกับบุคคลที่สามในการประมวลผลธุรกรรมเนื่องจากเงินของผู้ใช้จะถูกหักเป็นค่าธรรมเนียมการโอน ซึ่งในกรณีเช่นนี้ผู้ใช้ไม่สามารถรับรองความปลอดภัยของเงินตัวเองได้ เนื่องจากมีความเป็นไปได้สูงที่แฮ็กเกอร์ (Hacker) อาจขัดขวางเครือข่ายและขโมยเงินผู้ใช้ ด้วยเหตุนี้จึงเป็นที่มาของบล็อกเชน ซึ่งแทนที่จะใช้ธนาคารในการโอนเงิน หากผู้ใช้เลือกใช้บล็อกเชนในกรณีเช่นนี้ กระบวนการจะง่ายขึ้นและปลอดภัยขึ้นมาก และไม่มีค่าธรรมเนียมเพิ่มเติม เนื่องจากผู้ใช้เป็นผู้ดำเนินการโดยตรง ทำให้ไม่จำเป็นต้องใช้บุคคลที่สาม นอกจากนี้ฐานข้อมูลบล็อกเชนยังกระจายอำนาจและไม่จำกัดเพียงสถานที่เดียว หมายความว่า ข้อมูลและการบันทึกทั้งหมดที่เก็บไว้ในบล็อกเชนนั้น เป็นสาธารณะและกระจายอำนาจ เนื่องจากข้อมูลไม่ได้ถูกเก็บไว้ในที่เดียว แฮ็กเกอร์จึงไม่มีโอกาสสร้างความเสียหายแก่ข้อมูล (Singh, 2018)

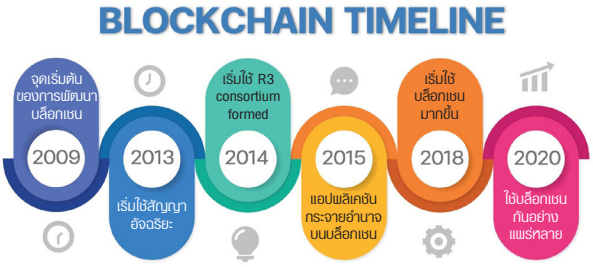
---

[2] Consensus หรือ ฉันทามติ เป็นข้อตกลงและความเห็นชอบร่วมกันระหว่างสมาชิกในเครือข่ายบล็อกเชน ทั้งนี้สมาชิกในเครือข่ายจะต้องยอมรับข้อตกลงร่วมกัน ด้วยกลไกในการควบคุมความถูกต้องของข้อมูลในทุกโหนด (Node) ผ่านอัลกอริทึม (Algorithm) ต่าง ๆ เพื่อให้ข้อมูลเป็นชุดเดียวกัน มีการจัดเก็บที่ตรงกัน

1.1.2 วิวัฒนาการของบล็อกเชน

บล็อกเชนมีจุดเริ่มต้นของเทคโนโลยีครั้งแรกในปี พ.ศ. 2551 (ค.ศ. 2008) โดยการนำเสนอของสตาโอชิ นากะโมโต (Staoshi Nakamoto, 2008) จากเอกสารงานวิจัยซึ่งเป็นการนำเสนอแนวคิดเกี่ยวกับการสร้างแพลตฟอร์ม (Platform) ที่สามารถสร้างความปลอดภัยในการแลกเปลี่ยนเงินสกุลดิจิทัล (Digital Currency) ที่มีชื่อว่า “บิตคอยน์ (Bitcoin)” โดยใช้ทฤษฎีเกี่ยวกับการทำคริปโทกราฟีและ Distributed Computing

ทั้งนี้วิวัฒนาการของบล็อกเชนเริ่มตั้งแต่การพัฒนาแอปพลิเคชันบล็อกเชน ซึ่งสามารถแบ่งออกเป็น 3 ช่วงใหญ่ ๆ ตามขั้นตอนของการพัฒนา ได้แก่ Blockchain 1.0, Blockchain 2.0 และ Blockchain 3.0



รูปที่ 1.2 วิวัฒนาการของบล็อกเชน
ที่มา : ผู้เขียน

จากรูปที่ 1.2 แสดงวิวัฒนาการของบล็อกเชน ได้แก่

ยุค Blockchain 1.0 เป็นจุดเริ่มต้นของการพัฒนาบล็อกเชน ซึ่งการพัฒนาในระยะที่ 1.0 ประกอบด้วยสกุลเงินแบบเสมือน หรือคริปโทเคอร์เรนซี (Cryptocurrency)[3] หรือเงินดิจิทัล เช่น บิตคอยน์ (Bitcoin) ซึ่งสามารถใช้แทนสกุลเงินจริงได้ เช่น ยูโรหรือดอลลาร์

ยุค Blockchain 2.0 คือ การใช้รูปแบบสัญญาอัจฉริยะหรือสมาร์ตคอนแทรกต์ (Smart Contract)[4] หมายถึงกระบวนการทางดิจิทัล ที่กำหนดขั้นตอนการทำธุรกรรมโดยอัตโนมัติไว้ล่วงหน้า โดยไม่ต้องอาศัยตัวกลาง อย่างเช่น ธนาคาร สถาบันการเงิน ทั้งการสร้างสมาร์ตคอนแทรกต์ที่เป็นระบบอัตโนมัติอย่างเต็มรูปแบบ โดยคู่สัญญาทั้งสองฝ่ายจะมีการตกลงกันก่อนหน้านี้ (Consensus) ถึงขั้นตอน กลไกในการทำรายการ ต่อมาวิวัฒนาการของบล็อกเชนในยุคปัจจุบันคือยุค Blockchain 3.0

---

[3] สกุลเงินดิจิทัล ซึ่งมีมูลค่าเหมือนกับธนบัตรในสกุลเงินประเทศต่าง ๆ และถูกใช้เป็นสื่อกลางในการแลกเปลี่ยนแบบดิจิทัล ยกตัวอย่างเช่น บิตคอยน์ (Bitcoin) และ Ripple
หมายเหตุ : Cryptocurrency ในหนังสือเล่มนี้จะใช้คำว่า คริปโทเคอร์เรนซี

[4] หมายเหตุ : Smart Contract ในหนังสือเล่มนี้จะใช้คำว่า สมาร์ตคอนแทรกต์หรือสัญญาอัจฉริยะ

ยุค Blockchain 3.0 คือ การพัฒนาแนวคิดเกี่ยวกับสมาร์ตคอนแทรกต์เพื่อสร้างกระบวนการแบบกระจายศูนย์ที่เป็นอิสระที่ต้องมีการกำหนดกฎการทำธุรกรรมของกลุ่มกันเองและดำเนินการด้วยความเป็นอิสระในรูปแบบธุรกรรมอัตโนมัติ จึงทำให้ Blockchain 3.0 สามารถขับเคลื่อนองค์กรดิจิทัลเต็มรูปแบบที่ไม่จำเป็นต้องมีพนักงานในการช่วยทำธุรกรรมเลยในอนาคต (เศรษฐพงค์ มะลิสุวรรณ, 2560)

1.1.3 คุณลักษณะของบล็อกเชน

คุณลักษณะของบล็อกเชน มีรายละเอียดดังนี้

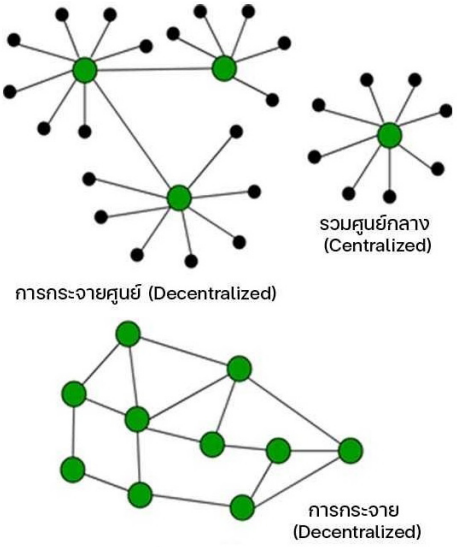
1. โครงสร้างการจัดเก็บข้อมูลของบล็อกเชน บล็อกเชนจะแตกต่างจากระบบฐานข้อมูลทั่วไป คือ มีวิธีการจัดโครงสร้างข้อมูลที่มีการรวบรวมข้อมูลเข้าด้วยกันเป็นกลุ่มที่เรียกว่า “บล็อก” ซึ่งมีชุดข้อมูลอยู่ โดยบล็อกมีความจุในการจัดเก็บที่แน่นอน และเมื่อเติมเต็มแล้วจะถูกโยงเข้ากับบล็อกที่เติมไว้ก่อนหน้านี้ ก่อตัวเป็นสายของข้อมูลที่เรียกว่า “บล็อกเชน”

จากรูปที่ 1.3 นำเสนอโครงสร้างการจัดเก็บข้อมูลของบล็อกเชน ซึ่งบล็อกเชนจะแตกต่างจากระบบฐานข้อมูลทั่วไป คือ มีวิธีการจัดโครงสร้างข้อมูลโดยการรวบรวมข้อมูลเข้าด้วยกันเป็นกลุ่มที่เรียกว่า “บล็อก” ซึ่งมีชุดข้อมูลอยู่ และบล็อกมีความจุในการจัดเก็บที่แน่นอน ซึ่งเมื่อเติมเต็มแล้วจะถูกโยงเข้ากับบล็อกที่เติมไว้ก่อนหน้านี้ ก่อตัวเป็นสายของข้อมูลที่เรียกว่า “บล็อกเชน” โดยข้อมูลใหม่ทั้งหมดที่ตามหลังบล็อกที่เพิ่มใหม่จะถูกรวบรวมเป็นบล็อกที่สร้างขึ้นใหม่ซึ่งจะถูกเพิ่มไปยังเชนและเมื่อเติมเสร็จแล้ว ฐานข้อมูลจัดโครงสร้างข้อมูลเป็นตาราง

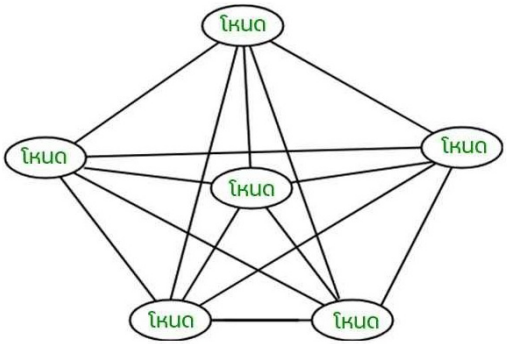
รูปที่ 1.3 โครงสร้างการจัดเก็บข้อมูลของบล็อกเชน

ทั้งนี้บล็อกเชนมีการจัดโครงสร้างข้อมูลเป็นชิ้น ๆ (บล็อก) ที่เชื่อมโยงเข้าด้วยกัน ซึ่งสิ่งนี้ทำให้บล็อกเชนทั้งหมดเป็นฐานข้อมูล แต่ไม่ใช่ทุกฐานข้อมูลที่เป็นบล็อกเชน อีกทั้งระบบนี้ยังสร้างไทม์ไลน์ (Timeline) ของข้อมูลที่ไม่สามารถย้อนกลับได้เมื่อนำไปใช้ในลักษณะการกระจายอำนาจ เมื่อบล็อกถูกเติม บล็อกจะถูกตั้งค่าและกลายเป็นส่วนหนึ่งของไทม์ไลน์นี้ และแต่ละบล็อกในสายโซ่จะได้รับการประทับเวลาที่แน่นอนเมื่อถูกเพิ่มเข้าไปในห่วงโซ่

ขณะที่รูปแบบของบล็อกเชน ซึ่งเป็นเครือข่ายแบบกระจายและมีความแตกต่างจากระบบประมวลผลแบบเดิมที่เป็นแบบรวมศูนย์กลาง (Centralized) และยังแสดงการเชื่อมต่อของโหนดในเครือข่ายบล็อกเชน จึงแสดงให้เห็นว่าแต่ละโหนดเองสามารถเชื่อมต่อกับโหนดอื่นได้หลายทาง ดังนั้นแม้ว่าการเชื่อมต่อในบางโหนดจะขาดช่วงไป การติดต่อและประมวลผลในระบบบล็อกเชนก็จะยังคงดำเนินต่อได้ บล็อกเชนเป็นเพียงกลุ่มบล็อกที่มีคุณสมบัติสำคัญ ๆ ซึ่งใช้เพื่อเปิดใช้งานการกระจายอำนาจทางอินเทอร์เน็ต โดยการกระจายอำนาจหมายความว่าไม่มีใครมีอำนาจเต็มหรือควบคุมเครือข่าย แต่มีการแจกจ่ายอำนาจให้กับผู้ใช้งานบนระบบ (Gupta, 2019)



รูปที่ 1.4 ลักษณะบล็อกเชนอยู่ในรูปแบบเครือข่ายของฐานข้อมูลเชิงกระจาย
ที่มา : ประยุกต์จาก Gupta (2019)



รูปที่ 1.5 บล็อกเชนคือเครือข่ายของโหนด
ที่มา : ผู้เขียน

2. คุณลักษณะพื้นฐานที่สำคัญของบล็อกเชน คุณลักษณะพื้นฐานที่สำคัญของการทำงานของบล็อกเชน 3 ประการ คือ ความถูกต้องเที่ยงตรงของข้อมูล (Data Integrity) ความโปร่งใสของข้อมูล (Data Transparency) และความสามารถในการทำงานได้อย่างต่อเนื่องของระบบ (Availability) (Serrano, 2017; สำนักงานพัฒนารัฐบาลอิเล็กทรอนิกส์, 2564) (ดังแสดงในรูปที่ 1.6)

(1) ความถูกต้องเที่ยงตรงของข้อมูล (Data Integrity) เนื่องจากบล็อกเชนได้ถูกเชื่อมโยงเข้าด้วยกันด้วยฟังก์ชันแฮช (Hash Function)[5] ที่กระจายให้ทุกโหนด ทำให้ข้อมูลที่บันทึกลงในบล็อกเชนแล้วไม่สามารถแก้ไขได้ หรือเปลี่ยนแปลงข้อมูลได้ (Immutability) ดังนั้นหากมีความพยายามที่จะบันทึกข้อมูลหรือแก้ไขข้อมูล จะทำให้ทราบได้ทันทีเนื่องจากข้อมูลในโหนดจะแตกต่างจากข้อมูลที่อยู่ในโหนดอื่นๆ ในระบบ และไม่สามารถสร้างฉันทามติ (Consensus) กับโหนดอื่นๆ ได้ ทำให้ถูกแยกออกจากโซ่ (Chain) หลักออกไป ซึ่งทำให้เกิดความถูกต้องเที่ยงตรงของข้อมูลที่อยู่บนระบบบล็อกเชน

รูปที่ 1.6 คุณลักษณะพื้นฐานที่สำคัญของบล็อกเชน
ที่มา : ผู้เขียน

(2) ความโปร่งใสของข้อมูล (Data Transparency) เกิดจากทุกโหนดในระบบบล็อกเชน จะเก็บข้อมูลชุดเดียวกันทั้งหมด ทำให้ไม่มีตัวกลางในการเก็บข้อมูลเพียงผู้เดียว จึงทำให้ผู้ใช้สามารถเข้าถึงข้อมูลจากโหนดได้ทันที ทำให้เกิดระบบที่มีความโปร่งใสของข้อมูลที่สูงมาก

(3) ความสามารถในการทำงานได้อย่างต่อเนื่องของระบบ (Availability) เนื่องจากทุกโหนดในระบบบล็อกเชนจะเก็บข้อมูลที่เหมือนกัน ทำให้หากเกิดเหตุฉุกเฉิน หรือสามารถใช้ข้อมูลจากทุกโหนดที่ใช้ทดแทนกันได้ โดยระบบบล็อกเชนจะสามารถคัดลอกสำเนาข้อมูลให้เป็นข้อมูลชุดเดียวกันเมื่อโหนดกลับขึ้นมาให้บริการได้อีกครั้ง ทำให้ระบบบล็อกเชนทำงานได้อย่างต่อเนื่อง

1.1.4 ลักษณะเฉพาะของบล็อกเชน

ปัจจุบันบล็อกเชนมีลักษณะการทำงานและลักษณะเฉพาะเหมือนกับบิตคอยน์ ซึ่งลักษณะเฉพาะของบล็อกเชน (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2564) ประกอบด้วย

1. Decentralized บล็อกเชนเป็นเครือข่ายแบบเพียร์ทูเพียร์ (Peer to Peer; P2P) ที่ทำงานแบบกระจายศูนย์ มีการประมวลผลของโหนดที่เป็นเครือข่ายเป็นอิสระต่อกัน โดยมีจุดประสงค์ในการกระจายอำนาจการประมวลผลข้อมูลไม่ให้ตกอยู่ในการควบคุมของบุคคลใดบุคคลหนึ่งหรือองค์กรใดองค์กรหนึ่ง

---

[5] Hash Function คือ การนำข้อมูลต้นฉบับที่ต้องการแปลงข้อมูลมาผ่านกระบวนการทางคณิตศาสตร์ ซึ่งเป็นฟังก์ชันทางเดียวในการแปลงข้อมูลให้อยู่ในรูปแบบที่มีลักษณะเฉพาะของข้อมูลและมีขนาดความยาวที่คงที่เสมอ โดยข้อมูลต้นฉบับที่ผ่านการทำ Hash Function แล้วจะไม่สามารถย้อนกลับเพื่อให้ได้ข้อมูลเดิมได้
หมายเหตุ : Hash Function ในหนังสือเล่มนี้จะใช้คำว่า ฟังก์ชันแฮช

2. Distributed Ledger บล็อกเชนมีการประมวลผลโครงสร้างข้อมูลที่เรียกว่าบัญชีแยกประเภท (Ledger) โดยแต่ละโหนดมีสำเนาบัญชีแยกประเภทเป็นของตัวเอง ประมวลผลบัญชีแยกประเภทด้วยตนเอง โดยโพรโทคอลในการทำฉันทามติเดียวกัน ข้อมูลธุรกรรมในบัญชีแยกประเภทมักจะบันทึกเป็นชุดที่เรียกว่า “บล็อก” ซึ่งแต่ละบล็อกจะเชื่อมต่อบล็อกก่อนหน้าโดยใช้การเก็บรหัสเป็นความลับ

3. Immutable เป็นกลไกรหัสลับทำให้ธุรกรรมที่ได้รับการบันทึกในบัญชีแยกประเภทแล้วจะย้อนคืน (Revert) ลบทิ้ง หรือเปลี่ยนแปลงไม่ได้ภายหลัง ดังนั้นบล็อกเชนจะรักษาความถูกต้องสมบูรณ์และความโปร่งใสของข้อมูลไว้ได้เป็นอย่างดี

4. Consensus บล็อกเชนมีการประมวลผลแบบ Decentralized ทำให้โหนดในเครือข่ายบล็อกเชนต้องมีโพรโทคอลในการทำฉันทามติ เพื่อประมวลผลบัญชีแยกประเภทที่จัดเก็บไว้ในแต่ละโหนดให้มีข้อมูลสอดคล้องตรงกัน

5. Openness บล็อกเชนสามารถเผยแพร่ระบบสารสนเทศ และใช้การพัฒนาซอฟต์แวร์ในรูปแบบโอเพนซอร์ซ (Opensource) เพื่อความโปร่งใส สร้างความน่าเชื่อถือในระบบ และเปิดโอกาสให้ทุกคนประเมินความน่าเชื่อถือของระบบได้

6. Anonymity ธุรกรรมบนบล็อกเชนมีเพียงที่อยู่ (เช่น Bitcoin Address) ที่ใช้อ้างอิงระหว่างกันเท่านั้น ไม่จำเป็นต้องมีข้อมูลที่ระบุตัวผู้ทำธุรกรรมได้ จึงสามารถรักษาความเป็นส่วนตัวของผู้ทำธุรกรรมได้

โดยสรุป บล็อกเชนเป็นเทคโนโลยีที่มีความปลอดภัยในการจัดเก็บข้อมูล และสามารถใช้ข้อมูลร่วมกันได้ของผู้ใช้งานบนระบบ หากจะมีการบันทึกข้อมูลหรือการปรับปรุงข้อมูลจะต้องได้รับการอนุญาตจากสมาชิกในเครือข่ายก่อนจึงจะปรับปรุงข้อมูลได้ วิวัฒนาการของบล็อกเชนเริ่มตั้งแต่การพัฒนาแอปพลิเคชันบล็อกเชน ซึ่งสามารถแบ่งออกเป็น 3 ช่วงใหญ่ ๆ ตามขั้นตอนของการพัฒนา ได้แก่ Blockchain 1.0, Blockchain 2.0 และปัจจุบันอยู่ในยุค Blockchain 3.0 ที่มีการใช้สมาร์ตคอนแทรกต์เพื่อสร้างกระบวนการแบบกระจายศูนย์ที่เป็นอิสระ จึงทำให้ Blockchain 3.0 สามารถขับเคลื่อนองค์กรดิจิทัลเต็มรูปแบบที่ไม่จำเป็นต้องมีพนักงานในการช่วยทำธุรกรรมเลยในอนาคต คุณลักษณะพื้นฐานที่สำคัญของการทำงานของบล็อกเชน 3 ประการ คือ ความถูกต้องเที่ยงตรงของข้อมูล (Data Integrity) ความโปร่งใสของข้อมูล (Data Transparency) และความสามารถในการทำงานได้อย่างต่อเนื่องของระบบ (Availability) อีกทั้งบล็อกเชนมีลักษณะการทำงานและลักษณะเฉพาะเหมือนกับบิตคอยน์ ซึ่งลักษณะเฉพาะของบล็อกเชน ได้แก่ (1) Decentralized (2) Distributed Ledger (3) Immutable (4) Consensus (5) Openness และ (6) Anonymity

1.2 สถาปัตยกรรมของบล็อกเชน (Blockchain Architecture)

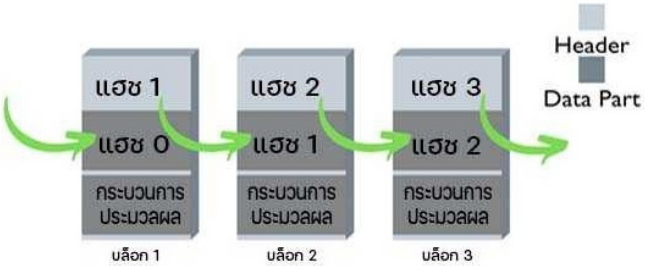
สถาปัตยกรรมของบล็อกเชน มีรายละเอียดดังนี้

1.2.1 องค์ประกอบของบล็อกเชน

ในการทำความเข้าใจว่า เทคโนโลยีบล็อกเชนแตกต่างจากแอปพลิเคชันไปจนถึงสกุลเงินดิจิทัลอย่างไร จำเป็นต้องเข้าใจองค์ประกอบเชิงตรรกะของระบบนิเวศบล็อกเชน (Blockchain Ecosystem) ซึ่งบล็อกเชนถูกแบ่งออกเป็น 4 องค์ประกอบ ได้แก่ (1) บล็อก (Block) (2) โซ่ (Chain) (3) ฉันทามติ (Consensus) และ (4) ความถูกต้อง (Validation)

รูปที่ 1.7 องค์ประกอบของบล็อกเชน
ที่มา : ผู้เขียน

1. บล็อก (Block) สำหรับเทคโนโลยีบล็อกเชน ข้อมูลจะถูกจัดเก็บไว้ในรูปแบบของ “บล็อก” โดยแต่ละบล็อกจะเชื่อมโยงเข้าหาบล็อกก่อนหน้าด้วยค่าฟังก์ชันแฮชของบล็อกก่อนหน้าเสมอ และจะเรียงต่อกันยาวในรูปแบบของโซ่ (Chain) ซึ่งรูปแบบของการทำงานบล็อกเชนนี้จะทำให้ยากต่อการปลอมแปลงข้อมูล อีกทั้งสามารถตรวจสอบความถูกต้องของข้อมูลได้ตลอดทั้งเชน (ดังแสดงในรูปที่ 1.8)



รูปที่ 1.8 องค์ประกอบภายในแต่ละบล็อกของบล็อกเชน
ที่มา : ประยุกต์จาก Ravi (2022)

องค์ประกอบของแต่ละบล็อก (Single Block) ของบล็อกเชนประกอบด้วย 7 ส่วน ได้แก่ (สำนักงานพัฒนารัฐบาลดิจิทัล, 2564)

(1) หมายเลขบล็อก คือตัวเลขใช้กำกับหมายเลขของบล็อก ซึ่งจะแสดงให้เห็นถึงตัวเลขบล็อกก่อนหลัง คือ บล็อกหมายเลข 1 จะเกิดขึ้นก่อนบล็อกหมายเลข 2 เป็นต้น

(2) การประทับเวลา (Timestamp)[6] ในระบบบล็อกเชนจะมีการประทับเวลา เพื่อให้ทราบเวลาที่บล็อกนี้ถูกสร้างขึ้น (CEO Channels, 2021)

(3) น็อนซ์ (Nonce)[7] คือค่าที่ใช้ในการค้นหาค่าแฮช (Hash) ของบล็อก ตามกฎของระบบที่ได้กำหนดไว้ ซึ่งกฎดังกล่าว คือ Proof of Work[8] หมายถึงหากต้องการจะสร้างบล็อกขึ้นมา จะต้องแสดงให้คนอื่นๆ ที่อยู่ในเครือข่ายบนระบบบล็อกเชนเห็นว่าได้แก้ปัญหาหรือทำงาน (Work) ตามกฎที่กำหนดไว้แล้ว

(4) Difficulty Target คือค่าระดับความยากที่จะถูกใช้ในการค้นหาค่าน็อนซ์ โดยค่าแฮชที่ได้นั้นจะต้องมีค่าต่ำกว่าค่า Difficulty Target

(5) Previous Hash ค่าแฮชของบล็อกก่อนหน้า (Previous Block's Hash Value) เรียกว่า Previous Block เป็นค่าแฮชของบล็อกก่อนหน้า ซึ่งทำให้ผู้ใช้รู้ว่าบล็อกนี้ต่อมาจากบล็อกใด ซึ่งค่าแฮชของบล็อกก่อนหน้าเปรียบได้กับค่า Digital Signature ของบล็อก ทั้งนี้หากมีการแก้ไขข้อมูลในบล็อกก่อนหน้าจะทำให้ค่าแฮชของบล็อกไม่เท่ากัน ทำให้ไม่สามารถประมวลผลได้ (Atcharanan, 2019)

(6) ข้อมูล (Data) คือข้อมูลที่ถูกบันทึกอยู่ในบล็อก

(7) Merkle Root คือค่าของแฮชของธุรกรรม (Transaction) ทั้งหมดในบล็อกซึ่งจะเป็นวิธีการแฮชข้อมูลชุดใหญ่ โดยใช้รูปแบบแฮชทรี (Hash Tree) ซึ่งธุรกรรมของแฮช (Hash Transaction) ทั้งหมดในบล็อก ให้กลายเป็น Hash Value[9] ขนาด 32 ไบต์

2. โซ่ (Chain) คือหลักการของการจดจำในการทำธุรกรรมของสมาชิกบนระบบเครือข่ายบล็อกเชน ที่สามารถบันทึกข้อมูลพร้อมกับจัดทำเป็นสำเนาบัญชีแยกประเภท แจกจ่ายให้กับ

---

6 หมายเหตุ : Timestamp ในหนังสือเล่มนี้จะใช้คำว่า การประทับเวลา

7 *หมายเหตุ : Nonce ในหนังสือเล่มนี้จะใช้คำว่า น็อนซ์

8 Proof of Work คือกระบวนการทำฉันทามติ (Consensus) โดยใช้การแก้ปัญหาทางคณิตศาสตร์ที่มีความซับซ้อนสูงจากโหนดต่างๆ ที่อยู่ในเครือข่ายบล็อกเชน หรือเรียกว่าไมเนอร์ส (Miners) เพื่อยืนยันความน่าเชื่อถือของข้อมูลที่จะถูกบันทึกลงในเครือข่าย ทั้งนี้ Miners จะได้รับค่าตอบแทนจากการทำ Proof of Work การแก้ไขข้อมูลในบล็อกเชนจึงทำได้ยาก

9 Hash Value คือค่าผลลัพธ์ที่ได้จากกระบวนการทำฟังก์ชันแฮช (Hash Function)

Hash Function คือการนำข้อมูลต้นฉบับที่ต้องการแปลงข้อมูลมาผ่านกระบวนการทางคณิตศาสตร์ซึ่งเป็นฟังก์ชันทางเดียวในการแปลงข้อมูลให้อยู่ในรูปแบบที่มีลักษณะเฉพาะของข้อมูลและมีขนาดความยาวที่คงที่เสมอ โดยข้อมูลต้นฉบับที่ผ่านการทำฟังก์ชันแฮช แล้วจะไม่สามารถย้อนกลับเพื่อให้ได้ข้อมูลเดิมได้

ทุกคนในระบบ โดยสำเนาบัญชีแยกประเภทจะถูกกระจายไปยังทุกโหนด เพื่อให้ทุกคนในระบบได้รับรู้ว่ากำลังทำธุรกรรมอะไรบ้าง (สำนักงานพัฒนาดิจิทัล, 2564)

รูปที่ 1.9 โครงสร้างภายในบล็อก
ที่มา : ประยุกต์จาก Nakamoto (2008)

3. กลไกฉันทามติ (Consensus) หมายถึง กลไกที่ควบคุมความถูกต้องของข้อมูลในทุกโหนดผ่านอัลกอริทึมต่างๆ เพื่อให้ข้อมูลมีความถูกต้อง เที่ยงตรงและเป็นข้อมูลชุดเดียวกัน รวมทั้งข้อมูลมีการจัดเก็บที่สอดคล้องและมีลำดับการจัดเก็บตรงกัน ผ่านการกำหนดข้อตกลงและความเห็นชอบของสมาชิกในเครือข่าย ซึ่งสมาชิกต้องยอมรับกฎระเบียบร่วมกัน ทั้งนี้กระบวนการฉันทามติมีอยู่ด้วยกันหลายวิธี โดยการเลือกใช้ฉันทามติวิธีใดนั้นขึ้นอยู่กับความเหมาะสมของบล็อกเชนในแต่ละประเภท

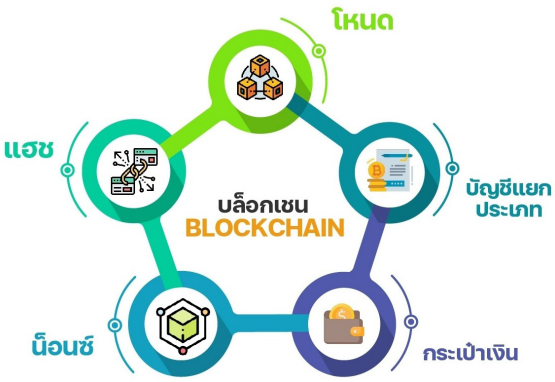
4. ความถูกต้อง (Validation) คือ การตรวจสอบความถูกต้องแบบทบทวนทั้งระบบและทุกโหนดในระบบบล็อกเชน เพื่อให้แน่ใจว่าจะไม่มีข้อผิดพลาดเกิดขึ้นไม่ว่าจะมาจากส่วนใดก็ตาม ซึ่งก็คือส่วนหนึ่งของฉันทามติ ที่เรียกว่า Proof of Work[10] ซึ่งเป็นส่วนหลักการแล้วทำการตรวจสอบความถูกต้อง

---

[10] Proof of Work เป็นกระบวนการทำฉันทามติ (Consensus) โดยใช้การแก้ปัญหาทางคณิตศาสตร์ซึ่งมีความซับซ้อนและต้องใช้เวลาในการแก้ไขปัญหานั้นๆ จากโหนดต่างๆ ในเครือข่ายที่เรียกว่า ไมเนอร์ (Miner) หรือผู้ขุด เพื่อยืนยันความน่าเชื่อถือของข้อมูลที่จะถูกบันทึกในเครือข่าย

1.2.2 ส่วนประกอบของเครือข่ายบล็อกเชน

ข้อมูลของบล็อกเชนจะถูกจัดเก็บในรูปแบบของบล็อก ทุกโหนดสามารถเห็นบล็อกได้ แต่ไม่สามารถเข้าไปยุ่งเกี่ยวกับบล็อกได้ หากค่าบล็อกถูกดัดแปลง ค่าแฮชที่เกี่ยวข้องกับการเปลี่ยนแปลงบล็อกนั้น และบล็อกนั้นจะถูกตัดการเชื่อมต่อจากเครือข่าย โดยเฉลี่ย 12.6 วินาที ทุกโหนดในเครือข่ายบล็อกเชนจะได้รับบล็อกเชนที่อัปเดตที่สุด โดยส่วนประกอบของเครือข่ายบล็อกเชน ประกอบไปด้วย (1) โหนด (Node) (2) บัญชีแยกประเภท (Ledger) (3) กระเป๋าเงิน (Wallet) (4) น็อนซ์ (Nonce) และ (5) แฮช (Hash) ดังรายละเอียดต่อไปนี้



รูปที่ 1.10 ส่วนประกอบของเครือข่ายบล็อกเชน
ที่มา : ผู้เขียน

1. โหนด (Node) มีสองประเภทคือ โหนดเต็มและโหนดบางส่วน

(1) โหนดเต็ม จะเก็บสำเนาธุรกรรมทั้งหมดไว้อย่างครบถ้วน มีความสามารถในการตรวจสอบ ยอมรับ และปฏิเสธธุรกรรม

(2) โหนดบางส่วน เรียกอีกอย่างว่า Lightweight Node เนื่องจากไม่ได้ดูแลสำเนาบัญชีแยกประเภทบล็อกเชนทั้งหมด จะรักษาเฉพาะค่าแฮชของธุรกรรม ซึ่งธุรกรรมทั้งหมดเข้าถึงได้โดยใช้ค่าแฮชนี้เท่านั้น โหนดเหล่านี้มีพื้นที่เก็บข้อมูลต่ำและมีกำลังในการคำนวณต่ำ

2. บัญชีแยกประเภท (Ledger) เป็นฐานข้อมูลของสกุลเงินดิจิทัล โดยบัญชีแยกประเภทมี 3 ประเภท ได้แก่

(1) บัญชีแยกประเภทสาธารณะ (Public Ledger) เปิดกว้างและโปร่งใสสำหรับทุกคนในเครือข่ายบล็อกเชนสามารถอ่านหรือเขียนอะไรบางอย่างได้

(2) บัญชีแยกประเภทแบบกระจาย (Distributed Ledger) ในบัญชีแยกประเภทนี้โหนดทั้งหมดมีสำเนาของฐานข้อมูลในเครื่อง ในที่นี้กลุ่มโหนดทำงานร่วมกัน เช่น ตรวจสอบธุรกรรม หรือเพิ่มบล็อกในบล็อกเชน

(3) บัญชีแยกประเภทแบบกระจายอำนาจ (Decentralized Ledger) ในบัญชีแยกประเภทนี้ ไม่มีโหนดหรือกลุ่มโหนดใดที่มีการควบคุมจากส่วนกลาง ทุกโหนดมีส่วนร่วมในการดำเนินงาน

3. กระเป๋าเงิน (Wallet) เป็นกระเป๋าเงินดิจิทัลที่ช่วยให้ผู้ใช้สามารถเก็บสกุลเงินดิจิทัลได้ โดยทุกโหนดในเครือข่ายบล็อกเชนมีกระเป๋าเงิน โดยกระเป๋าเงินคริปโทเคอร์เรนซีส่วนใหญ่มีสองประเภท คือ

(1) กระเป๋าเงินร้อน (Hot Wallet) กระเป๋าเงินเหล่านี้ใช้สำหรับการทำธุรกรรมออนไลน์แบบวันต่อวันที่เชื่อมต่อกับอินเทอร์เน็ต แฮ็กเกอร์สามารถโจมตีกระเป๋าเงินนี้ได้เมื่อเชื่อมต่อกับอินเทอร์เน็ต โดยกระเป๋าเงินร้อนแบ่งออกเป็นสองประเภทเพิ่มเติม ได้แก่

- กระเป๋าเงินออนไลน์/เว็บ (Online/ Web Wallet) กระเป๋าเงินเหล่านี้ทำงานบนแพลตฟอร์มคลาวด์ ตัวอย่างเช่น กระเป๋าเงิน MyEther และกระเป๋าเงินเมตามาสก์ (MetaMask)
- กระเป๋าซอฟต์แวร์ (Software Wallet) ประกอบด้วยกระเป๋าเงินเดสก์ท็อป (Desktop Wallet) และกระเป๋าเงินมือถือ กระเป๋าเงินเดสก์ท็อปสามารถดาวน์โหลดได้บนเดสก์ท็อปและผู้ใช้จะสามารถควบคุมกระเป๋าเงินทั้งหมดได้ ตัวอย่างของกระเป๋าเงินเดสก์ท็อป คือ Electrum
- กระเป๋าเงินมือถือ (Mobile Wallet) เป็นกระเป๋าเงินที่ออกแบบมาเพื่อใช้งานบนอุปกรณ์สมาร์ตโฟน

(2) กระเป๋าเงินเย็น (Cold Wallet) กระเป๋าเงินเหล่านี้ไม่ได้เชื่อมต่อกับอินเทอร์เน็ต ซึ่งปลอดภัยมากและแฮ็กเกอร์ไม่สามารถโจมตีได้ กระเป๋าเงินเหล่านี้ซื้อโดยผู้ใช้ ตัวอย่างเช่น Paper Wallet และ Hardware Wallet เป็นต้น

- กระเป๋าเงินกระดาษ (Paper Wallet) เป็นกระเป๋าเงินออฟไลน์ที่ใช้แผ่นกระดาษที่มีที่อยู่การเข้ารหัสลับ รหัสส่วนตัวถูกพิมพ์ในรูปแบบรหัส QR โดยรหัส QR ถูกสแกนสำหรับธุรกรรมสกุลเงินดิจิทัล
- กระเป๋าเงินฮาร์ดแวร์ (Hardware Wallet) เป็นอุปกรณ์อิเล็กทรอนิกส์ทางกายภาพที่ใช้ตัวสร้างตัวเลขสุ่มที่เกี่ยวข้องกับกระเป๋าเงิน

ทั้งนี้จุดที่น่าสนใจของกระเป๋าเงินอยู่ที่สามสิ่งนี้ได้แก่ (1) ความเป็นส่วนตัว (2) การทำธุรกรรมควรมีความปลอดภัย และ (3) ง่ายต่อการใช้ ซึ่งการรักษาความเป็นส่วนตัวของกระเป๋าเงินจะใช้คู่คีย์สาธารณะและส่วนตัว ธุรกรรมได้รับการรักษาความปลอดภัยเนื่องจากใช้คีย์ส่วนตัวทั้งในการส่งเงินและเพื่อเปิดข้อความที่เข้ารหัส

(1) น็อนซ์ (Nonce) เป็นตัวย่อของ “ตัวเลขที่ใช้เพียงครั้งเดียว” ซึ่งเป็นตัวเลขที่เพิ่มลงในบล็อกที่แฮช หรือเข้ารหัสในบล็อกเชน เป็นหมายเลข 32 บิตที่สร้างขึ้นแบบสุ่มเพียงครั้งเดียวที่ช่วยในการสร้างบล็อกใหม่ หรือตรวจสอบความถูกต้องของธุรกรรม ใช้เพื่อทำให้การทำธุรกรรมมีความปลอดภัยมากขึ้น

(2) แฮช (Hash) มีบทบาทสำคัญในการเข้ารหัส ในค่าแฮชเครือข่ายบล็อกเชนของธุรกรรมหนึ่งเป็นการป้อนข้อมูลของอีกธุรกรรมหนึ่ง โดยคุณสมบัติของฟังก์ชันแฮชมีดังนี้ (1) ทนต่อการชน (Collision Resistant) (2) ซ่อนข้อมูล และ (3) ใช้งานง่าย (Puzzle Friendliness)

โดยสรุป บล็อกเชนเป็นเทคโนโลยีการประมวลผลและจัดเก็บข้อมูลแบบกระจายศูนย์ (Distributed Ledger Technology; DLT) เป็นรูปแบบการบันทึกข้อมูลที่ใช้หลักการคริปโทกราฟีร่วมกับกลไกฉันทามติ ทำให้ข้อมูลที่ถูกบันทึกไปแล้วสามารถเปลี่ยนแปลงหรือแก้ไขได้ยาก เพิ่มความถูกต้องเชื่อถือได้ โปร่งใส และสามารถปรับปรุงข้อมูลได้ โดยวิวัฒนาการของบล็อกเชนเริ่มตั้งแต่การพัฒนาแอปพลิเคชันบล็อกเชนตามขั้นตอนของการพัฒนา ได้แก่ Blockchain 1.0, Blockchain 2.0 และในปัจจุบันก้าวสู่ Blockchain 3.0 โดยบล็อกเชนมีองค์ประกอบที่สำคัญ 4 ส่วน ได้แก่ (1) บล็อก (2) โซ่ (3) ฉันทามติ และ (4) ความถูกต้อง และส่วนประกอบของเครือข่ายบล็อกเชนประกอบไปด้วย (1) โหนด (2) บัญชีแยกประเภท (3) กระเป๋าเงิน (4) น็อนซ์ และ (5) แฮช

1.2.3 สถาปัตยกรรมของบล็อกเชน (Blockchain Architecture)

สถาปัตยกรรมของบล็อกเชนซึ่งมีลักษณะการทำงานเป็นเลเยอร์ (Layer) ภายในดังแสดงในรูปที่ 1.11

1. เครือข่าย (Network) เป็นเลเยอร์ต่ำสุดคือ Network ซึ่งมักจะเป็นอินเทอร์เน็ตและไอซีพี/ไอพี (ICP/IP) ที่จะเป็นพื้นฐานและจัดเตรียมเลเยอร์การสื่อสารพื้นฐานสำหรับบล็อกเชน

2. เพียร์ทูเพียร์ (P2P) เครือข่าย P2P ทำงานบนเลเยอร์เครือข่ายซึ่งประกอบด้วยข้อมูลโพรโทคอลการแพร่กระจาย เช่น Routing Protocols และ Folding Protocols

3. คริปโทกราฟี (Cryptography) หลังจากนี้มาถึงเลเยอร์การเข้ารหัสซึ่งมีโพรโทคอลการเข้ารหัสที่สำคัญ สำหรับการรับรองความปลอดภัยของบล็อกเชน โพรโทคอลการเข้ารหัสเหล่านี้มีความสำคัญ และมีบทบาทในการรักษาความปลอดภัยและความสมบูรณ์ของกระบวนการบล็อกเชน โดยเลเยอร์นี้ประกอบด้วยการเข้ารหัสคีย์สาธารณะและส่วนประกอบที่เกี่ยวข้อง เช่น ลายเซ็นดิจิทัล และฟังก์ชันแฮชเข้ารหัส

4. ฉันทามติ (Consensus) ในเลเยอร์นี้มีส่วนสำคัญของสถาปัตยกรรมบล็อก ซึ่งประกอบด้วยเทคนิคต่าง ๆ เช่น SMR Consensus ตามหลักฐาน (Proof Based Consensus

Mechanism) หรือแบบดั้งเดิม (Traditional) จากการวิจัยระบบกระจายแบบดั้งเดิมมักใช้ฉันทามติที่ทนต่อข้อผิดพลาดของไบแซนไทน์โพรโทคอล (Byzantine Fault–tolerant)

5. การดำเนินการ (Execution) นอกจากนี้มีเลเยอร์การดำเนินงาน ซึ่งสามารถประกอบด้วยเครื่องเสมือน (Virtual Machine) บล็อก ธุรกรรม และสัญญา (Contract)

6. แอปพลิเคชัน (Applications) สุดท้ายมีเลเยอร์แอปพลิเคชัน ซึ่งประกอบด้วยสมาร์ตคอนแทรกต์แอปพลิเคชันแบบกระจายศูนย์ DAO และตัวแทนอิสระ (Autonomous Agents) ชั้นนี้ได้อย่างมีประสิทธิภาพ มีตัวแทนระดับผู้ใช้ที่หลากหลายและโปรแกรมที่ทำงานบนบล็อกเชนผู้ใช้โต้ตอบกับบล็อกเชนผ่านแอปพลิเคชันที่กระจายอำนาจ

รูปที่ 1.11 สถาปัตยกรรมบล็อกเชน
ที่มา : ประยุกต์จาก Bashir (2018)

โดยสรุป สถาปัตยกรรมของบล็อกเชนมีการทำงานเป็นชั้นหรือเลเยอร์ ซึ่งประกอบด้วยชั้นนอกที่ติดต่อกับอินเทอร์เน็ตเริ่มจากชั้นเครือข่าย (Network) เชื่อมต่อกับ P2P และเข้าสู่ชั้นคริปโทกราฟี (Cryptography) ซึ่งจะเริ่มเข้าสู่กระบวนการในบล็อกเชน และเข้าสู่ชั้นฉันทามตินำมาสู่การประมวลผล และทำงานในชั้นแอปพลิเคชันชั้นในสุด

1.3 การทำงานของบล็อกเชน

การทำงานของบล็อกเชน มีดังนี้

1.3.1 การทำงานของบล็อกเชน

ด้วยหลักการทำงานของเทคโนโลยีบล็อกเชนเป็นเทคโนโลยีการประมวลผลและจัดเก็บข้อมูลแบบกระจายศูนย์ (DLT) กระจายข้อมูลจัดเก็บไปยังเครื่องคอมพิวเตอร์หรือโหนดที่เชื่อมโยงกันในเครือข่ายบล็อกเชน จึงทำให้การจัดเก็บข้อมูลสามารถมีเพียงข้อมูลชุดเดียวโดยไม่จำเป็นต้องมีตัวกลางในการควบคุม และลดความเสี่ยงจากการถูกปลอมแปลงข้อมูล นอกจากนี้ยังช่วยให้สามารถทำธุรกรรมแบบอัตโนมัติผ่านสัญญาอัจฉริยะหรือสมาร์ตคอนแทรกต์ (Smart Contract)[11] เนื่องจากหากเกิดกรณีที่มีการเปลี่ยนแปลงแก้ไขข้อมูลธุรกรรม การเปลี่ยนแปลงนั้นจะต้องได้รับการตรวจสอบและลงความเห็นจากสมาชิกในเครือข่าย (การทำฉันทามติ) ส่งผลให้การบริหารจัดการข้อมูลในเครือข่ายบล็อกเชนมีความปลอดภัย น่าเชื่อถือ และยากต่อการแก้ไขหากไม่ได้รับอนุญาต ทั้งนี้กระบวนการทำงานพื้นฐานที่สำคัญของเทคโนโลยีบล็อกเชนประกอบด้วยขั้นตอนหลัก (ดังแสดงในรูปที่ 1.12)

1. สร้างคำสั่งธุรกรรม (Create) สำหรับส่งข้อมูลและคำสั่งเพื่อทำธุรกรรมที่เกี่ยวข้อง เช่น โอนเงิน ซื้อขายพันธบัตร โดยส่งผ่าน Endpoint และจุดเชื่อมต่อที่เป็นระบบโครงสร้างพื้นฐานเดิม ผ่าน API2 ไปประมวลยังสมาร์ตคอนแทรกต์ภายในโหนด

2. ประมวลผลและส่งต่อข้อมูล (Process and Broadcast) เพื่อให้โหนดในเครือข่ายบล็อกเชนที่เกี่ยวข้องกับคำสั่งธุรกรรมได้บันทึกข้อมูลลงในบล็อก และอาจประมวลผลพร้อมทั้งตรวจสอบข้อมูลร่วมกันด้วย

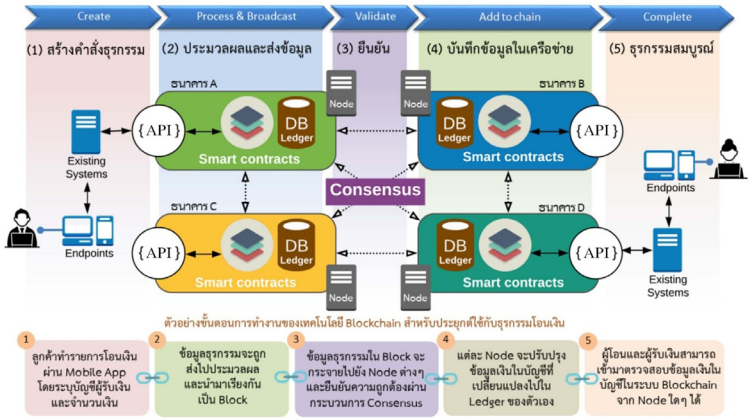
3. ยืนยันและตรวจสอบข้อมูล (Validate) ผ่านการลงความเห็นจากสมาชิกในเครือข่ายที่ได้รับมอบหมายโดยเป็นไปตามรูปแบบของฉันทามติในเครือข่าย

4. บันทึกข้อมูลในเครือข่าย (Add to Chain) โดยนำบล็อกมาเชื่อมต่อกับบล็อกก่อนหน้าในรูปแบบโซ่หรือเชน หรือเป็นไปตามการออกแบบในแต่ละประเภทของแพลตฟอร์มบล็อกเชน

5. ธุรกรรมสมบูรณ์ (Complete) ข้อมูลมีความน่าเชื่อถือ ยากต่อการเปลี่ยนแปลง สามารถใช้อ้างอิงในการดำเนินธุรกรรมต่อไป

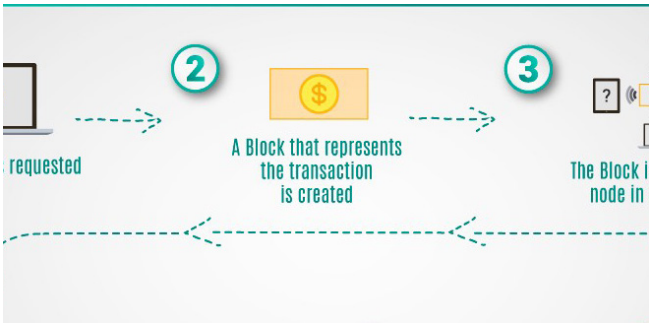
---

[11] สมาร์ตคอนแทรกต์ (Smart Contract) หมายถึง สัญญาอัจฉริยะ โดยจัดเก็บเงื่อนไขหรือข้อตกลงของสัญญาต่าง ๆ ไว้ในรูปแบบโปรแกรมคอมพิวเตอร์ ซึ่งจะถูกจัดเก็บและดำเนินการ (Execute) ในเครือข่ายบล็อกเชน
หมายเหตุ : สัญญาอัจฉริยะ ในหนังสือเล่มนี้จะใช้คำว่า สมาร์ตคอนแทรกต์ (Smart Contract)



รูปที่ 1.12 การทำงานของบล็อกเชน
ที่มา : ประยุกต์จากธนาคารแห่งประเทศไทย (2563)

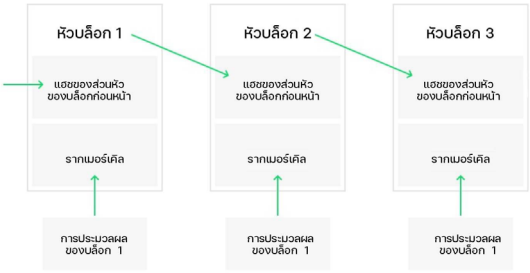
ในขณะที่ธุรกรรมเกิดขึ้นบนบล็อกเชน มีโหนดบนเครือข่ายที่ตรวจสอบธุรกรรมเหล่านี้ในบล็อกเชนของบิตคอยน์ โดยโหนดเหล่านี้เรียกว่า เป็นผู้ขุด[12] (Miner) และใช้แนวคิดของการพิสูจน์การทำงานเพื่อประมวลผลและตรวจสอบธุรกรรมบนเครือข่าย เพื่อให้ธุรกรรมถูกต้อง โดยแต่ละบล็อกต้องอ้างอิงถึงค่าแฮช (Hash) ของบล็อกก่อนหน้า การทำธุรกรรมจะเกิดขึ้นก็ต่อเมื่อแฮชถูกต้องเท่านั้น หากแฮ็กเกอร์พยายามโจมตีเครือข่ายและเปลี่ยนแปลงข้อมูลของบล็อกใดๆ เฉพาะแฮชที่ติดอยู่กับบล็อกนั้นก็จะได้รับการแก้ไขเช่นกัน การละเมิดจะถูกตรวจพบเนื่องจากแฮชที่แก้ไขจะไม่ตรงกับแฮชดั้งเดิม ซึ่งทำให้มั่นใจได้ว่าบล็อกเชนจะไม่สามารถแก้ไขได้ ราวกับว่าการเปลี่ยนแปลงใดๆ ที่เกิดขึ้นกับบล็อกเชนจะสะท้อนให้เห็นทั่วทั้งเครือข่ายและจะถูกตรวจจับได้ง่าย (MLSDev, 2019)



รูปที่ 1.13 การทำงานของบล็อกเชน
ที่มา : ประยุกต์จาก MLSDev (2019)

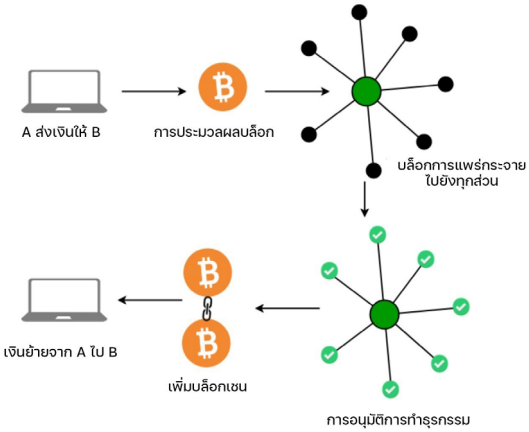
[12] การขุดบล็อก หมายถึง การเพิ่มบล็อกที่มีอยู่ในเครือข่ายบล็อกเชน นักขุดจะเลือกชุดของธุรกรรมจากกลุ่มของธุรกรรมจากนั้นจึงขุดบล็อก หรืออาจกล่าวได้ว่า คำนวณค่าแฮช (Hash) เพื่อเพิ่มบล็อกลงในเครือข่าย หากนักขุดสองคนหรือมากกว่าขุดบล็อกเดียวกันพร้อมกัน บล็อกที่ยากกว่าจะถูกเลือกก่อน ซึ่งคนอื่นๆ จะเรียกว่าบล็อกเก่า โดยการขุดมักจะให้รางวัลแก่นักขุดด้วยสกุลเงินบล็อกเชน (Gupta, 2019)

จากรูปที่ 1.13 แสดงการทำงานของบล็อกเชน ซึ่งมีรายละเอียดดังนี้



รูปที่ 1.14 แสดงความสัมพันธ์ของแต่ละบล็อกในบล็อกเชน
ที่มา : ประยุกต์จาก MLSDev (2019)

ทั้งนี้เพื่อให้เห็นภาพของบล็อกเชนได้ชัดขึ้น รูปที่ 1.14 อธิบายความสัมพันธ์ของแต่ละบล็อกที่เกิดขึ้นในเครือข่ายบล็อกเชน แสดงให้เห็นว่าแต่ละส่วนหัวของบล็อก (Block Header) จะมีการลิงก์ไปยังแฮชของส่วนหัวของบล็อกก่อนหน้า (Previous Block Header) ซึ่งการเชื่อมโยงนี้เองที่เรียกว่าเชน (Chain) (Gupta, 2019)



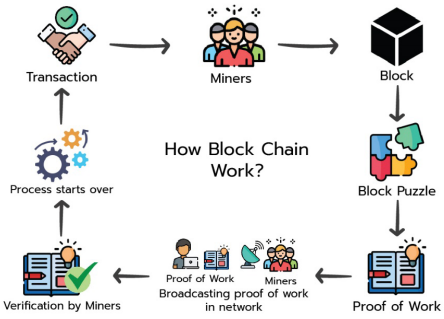
รูปที่ 1.15 แสดงการโอนเงินจาก A ไป B ผ่านเครือข่ายบล็อกเชน
ที่มา : ประยุกต์จาก Singh (2018)

จากรูปที่ 1.15 แสดงตัวอย่างของการทำธุรกรรมโดยใช้บล็อกเชน โดยมีการโอนเงินจากผู้ใช้ A ไปยังผู้ใช้ B ผ่านเครือข่ายบล็อกเชน ซึ่งบล็อกของธุรกรรม หรือธุรกรรมจะถูกเผยแพร่ (Broadcast) ออกไปทั้งเครือข่ายเพื่อให้แต่ละโหนดในเครือข่ายช่วยกันอนุมัติธุรกรรม ซึ่งกระบวนการรับรองการทำธุรกรรมด้วยโหนดบนเครือข่ายบล็อกเชนนี้ สามารถนำไปเพิ่มความน่าเชื่อถือในการรับรู้ข่าวสารจากแหล่งข้อมูล

ทั้งนี้จากการทำงานของระบบบล็อกเชน ผู้เขียนได้มีการนำมาประยุกต์ใช้กับการท่องเที่ยวอัจฉริยะ (Smart Tourism) ในการดำเนินโครงการวิจัยของผู้เขียนที่นำเทคโนโลยีบล็อกเชนมาประยุกต์ใช้กับการท่องเที่ยวอัจฉริยะในจังหวัดสุพรรณบุรี เพื่อใช้สำหรับการสนับสนุนการทำธุรกรรมทางการเงินของแหล่งท่องเที่ยวชุมชน เป็นต้น (Suanpang et al., 2021)

1.4 การทำธุรกรรมในบล็อกเชน

จากแนวคิดของบล็อกเชนที่กล่าวมาข้างต้น สามารถสรุปวิธีที่บล็อกเชนช่วยให้การทำธุรกรรมเกิดขึ้นได้ดังนี้ (Singh, 2018)



รูปที่ 1.16 วิธีการทำธุรกรรมของบล็อกเชน
ที่มา : ประยุกต์จาก Singh (2018)

วิธีการทำธุรกรรมของบล็อกเชน (ดังแสดงในรูปที่ 1.16) โดยเริ่มจาก

1. การตกลงที่จะทำธุรกรรมร่วมกัน

2. ส่งข้อมูลไปยังบล็อก

3. โดยเครือข่ายบล็อกเชนใช้คีย์สาธารณะและคีย์ส่วนตัวเพื่อสร้างลายเซ็นดิจิทัลเพื่อรับรองความปลอดภัยและความยินยอม เมื่อรับรองความถูกต้องผ่านคีย์เหล่านี้แล้ว

4. จำเป็นต้องมีการอนุญาต ผ่าน Block Puzzle ในขณะทำการโอน ผู้ส่งจะใช้คีย์ส่วนตัวและประกาศข้อมูลธุรกรรมผ่านเครือข่าย มีการสร้างบล็อกที่มีข้อมูล เช่น ลายเซ็นดิจิทัล การประทับเวลา และคีย์สาธารณะของผู้รับ

5. นักขุดทั่วทั้งเครือข่ายเริ่มไขปริศนาทางคณิตศาสตร์ที่เกี่ยวข้องกับธุรกรรมเพื่อดำเนินการเมื่อไขปริศนาได้ก่อน ผู้ขุดจะได้รับรางวัลเป็นบิตคอยน์ ปัญหาประเภทนี้เรียกว่า **ปัญหาทางคณิตศาสตร์ที่พิสูจน์การทำงาน (Proof of Work)**

6. เมื่อโหนดส่วนใหญ่ในเครือข่ายได้รับฉันทามติและตกลงที่จะแก้ไขปัญหาร่วมกัน บล็อกนั้นจะถูกประทับเวลาและเพิ่มไปยังบล็อกเชนที่มีอยู่ ซึ่งบล็อกนี้สามารถมีอะไรก็ได้ตั้งแต่เงินไปจนถึงข้อมูลและส่งถึงข้อความ

7. หลังจากที่บล็อกใหม่ถูกเพิ่มเข้าไปในเชน สำเนาของบล็อกเชนที่มีอยู่จะได้รับการอัปเดตสำหรับโหนดทั้งหมดในเครือข่าย

โดยสรุป การทำงานของบล็อกเชนเริ่มตั้งแต่การกำหนดธุรกรรม ส่งข้อมูลลงในบล็อก และทำการตรวจสอบ ส่งข้อมูลไปจัดเก็บลงในโหนด และเสร็จสิ้นกระบวนการ

1.5 การจำแนกประเภทของบล็อกเชน

หากพิจารณาจากโครงสร้างแล้ว สามารถจำแนกโครงข่ายบล็อกเชนออกเป็น 3 ประเภท คือ (1) บล็อกเชนสาธารณะ (Public Blockchain) (2) บล็อกเชนส่วนตัว (Private Blockchain) และ (3) บล็อกเชนเฉพาะกลุ่ม (Consortium Blockchain) โดยรูปที่ 1.17 แสดงความแตกต่างระหว่างบล็อกเชนสาธารณะ และบล็อกเชนส่วนตัว และตารางที่ 1.1 การเปรียบเทียบบล็อกเชนทั้ง 3 ประเภท (Kohut, 2018)

1.5.1 บล็อกเชนสาธารณะ (Public Blockchain)

บล็อกเชนสาธารณะนั้นไม่ได้รับอนุญาตให้ทุกคนเข้าร่วมและมีการกระจายอำนาจอย่างสมบูรณ์ โดยบล็อกเชนสาธารณะอนุญาตให้โหนดทั้งหมดของบล็อกเชนมีสิทธิ์เท่าเทียมกันในการเข้าถึงบล็อกเชน สร้างบล็อกข้อมูลใหม่ และตรวจสอบบล็อกของข้อมูล

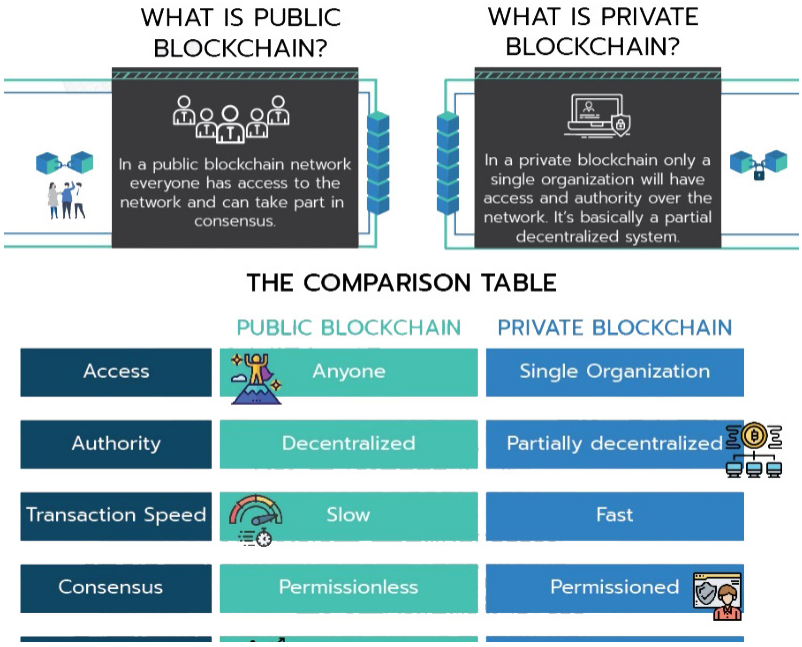
1.5.2 บล็อกเชนส่วนตัว (Private Blockchain)

บล็อกเชนส่วนตัว ซึ่งอาจเรียกได้ว่าเป็นบล็อกเชนที่มีการจัดการที่ได้รับอนุญาต โดยมีการควบคุมโดยองค์กรเดียวในบล็อกเชนส่วนตัว ซึ่งผู้มีอำนาจส่วนกลางจะกำหนดว่าใครสามารถเป็นโหนดได้โดยผู้มีอำนาจส่วนกลางไม่จำเป็นต้องให้แต่ละโหนดมีสิทธิ์เท่าเทียมกันในการปฏิบัติหน้าที่ บล็อกเชนส่วนตัวมีการกระจายอำนาจเพียงบางส่วนเท่านั้นเนื่องจากการเข้าถึงบล็อกเชนเหล่านี้ ถ้าเป็นแบบสาธารณะจะถูกจำกัดตัวอย่างบางส่วนของบล็อกเชนส่วนตัว ได้แก่ เครือข่ายการแลกเปลี่ยนสกุลเงินเสมือนระหว่างธุรกิจกับธุรกิจ Ripple และ Hyperledger ซึ่งเป็นโครงการของแอปพลิเคชันบล็อกเชนแบบโอเพนซอร์ซ เป็นต้น

1.5.3 บล็อกเชนเฉพาะกลุ่ม (Consortium Blockchain)

บล็อกเชนเฉพาะกลุ่ม เป็นบล็อกเชนที่เปิดใช้งานเฉพาะกลุ่มเท่านั้น ซึ่งเป็นการผสมผสานแนวคิดของบล็อกเชนสาธารณะ และบล็อกเชนส่วนตัวเข้าด้วยกัน ทั้งนี้การทำธุรกรรมแบบกลุ่มบล็อกเชนในรูปแบบองค์กรที่มีการแลกเปลี่ยนข้อมูลระหว่างกันอย่างสม่ำเสมออยู่แล้วมารวมตัวกันตั้งวงบล็อกเชนขึ้นมา เนื่องจากธุรกรรมและข้อมูลที่จัดเก็บบนระบบเป็นความลับ

หรือเป็นข้อมูลส่วนตัวภายในองค์กร ส่งผลให้ไม่สามารถเปิดเผยข้อมูลนั้นสู่สาธารณะได้ ดังนั้น ผู้เข้าร่วมเฉพาะกลุ่มบล็อกเชน จำเป็นต้องได้รับอนุญาตจากตัวแทนเสียก่อนจึงจะสามารถเข้าใช้งานได้ (สำนักงานพัฒนาดิจิทัล, 2564)



รูปที่ 1.17 ประเภทของบล็อกเชน
ที่มา : ประยุกต์จาก Iredale (2021)

ตารางที่ 1.1 การเปรียบเทียบบล็อกเชน

คุณสมบัติ	Private Blockchain	Public Blockchain	Permissionless[13] (Public Blockchain)
ผู้มีอำนาจ (Authority) การควบคุม (Control) ความน่าเชื่อถือ (Trust)	บริหารจัดการบัญชีแยกประเภทไว้ในองค์กรเดียว (Centralized Trust)	การจัดการบัญชีแยกประเภทโดยมีประโยชน์ของอุตสาหกรรมเป็นสำคัญ และเปิดการใช้งานแบบสาธารณะ	การจัดการบัญชีแยกประเภท โดยเครือข่ายแบบกระจายศูนย์ไม่มีระบบข้อมูลกลาง (Distributed Consensus)
บริบททางธุรกิจ (Business Context)	ใช้งานภายในองค์กรเท่านั้น	ใช้งานระหว่างองค์กร	ใช้งานสำหรับบริษัทและบุคคลทั่วไป สาธารณะที่อยู่ระหว่างเครือข่ายหรือระบบนิเวศของบล็อกเชน
สิทธิ์ในการเข้าถึง (Access Rights)	สิทธิ์การใช้งานวัตถุประสงค์เดียวของหนึ่งองค์กร	กำหนดสิทธิในอุตสาหกรรมหลายแบบ	อนุญาตให้ผู้เข้าร่วมหลายอุตสาหกรรมและรองรับผู้ที่ต้องการใช้งานหลายประเภท
การเป็นสมาชิก (Membership)	Static	Semi-static	Fluid

ตารางที่ 1.1 (ต่อ) การเปรียบเทียบบล็อกเชน

คุณสมบัติ	Private Blockchain	Public Blockchain	Permissionless[13] (Public Blockchain)
ความรับผิดชอบ (Accountability) สถานะทางกฎหมาย	ผู้รับผิดชอบตามกฎหมาย	ผู้รับผิดชอบตามกฎหมายและอาจได้รับการควบคุม	ผู้รับผิดชอบตามกฎหมายจำกัด/ไม่มีกฎหมายรับรองและผู้ใช้ไม่ได้รับการควบคุม
รูปแบบการนำไปใช้ (Deployment Style)	อาจแก้ไขได้	แก้ไขได้	ส่วนใหญ่ไม่สามารถแก้ไขได้
บันทึกการเปลี่ยนแปลงไม่ได้ (Record Immutability)	อาจแก้ไขได้	แก้ไขได้	ส่วนใหญ่ไม่สามารถแก้ไขได้
กลไกฉันทามติ (Consensus Mechanism)	Ethereum Kovan Testnet, POA Chain, R3 (Banks), EWF (Energy), B3i (Insurance), Corda		Bitcoin, Ethereum, etc.
ข้อดี (Advantage)	1. การรองรับความถูกต้องและการรักษาความปลอดภัยมีความน่าเชื่อถือ 2. สามารถปรับปรุงหรือเพิ่มประสิทธิภาพของเครือข่ายได้ 3. ประหยัดค่าใช้จ่ายในการจัดการระบบเครือข่าย 4. สามารถบังคับใช้นโยบายและกำกับดูแลระบบเครือข่ายได้ 5. สามารถปฏิบัติตามกฎระเบียบได้ 6. สามารถพัฒนามาตรฐานและการควบคุมได้ 7. มีประสิทธิภาพในการทำงานที่รวดเร็ว 8. ปกป้องข้อมูลให้มีความมั่นคงและปลอดภัยได้		1. ข้อมูลทั้งหมดจะเป็นสาธารณะ 2. มีความสามารถในการป้องกันการถูกโจมตี 3. ไม่มีศูนย์กลางในการควบคุม 4. ไม่มีการแยกผู้ใช้ออกจากนักพัฒนาระบบ 5. การเติบโตของระบบนิเวศผ่านทางเครือข่าย 6. โอเพนซอร์ซ (Opensource) 7. สามารถมีนักพัฒนาระบบร่วมกันในเครือข่ายได้
ข้อเสีย (Disadvantage)	1. มีความเสี่ยงต่อการล้มเหลวในการทำธุรกรรม (Single Point Failure) 2. อาจไม่สามารถเปิดแหล่งที่มาได้ 3. เสริมสร้างรูปแบบธุรกิจ 4. บุคลากรทางด้านการพัฒนาซอฟต์แวร์มีอยู่จำกัด 5. การใช้งานต้องมีฉันทามติหรือข้อตกลงเป็นเอกฉันท์ขององค์กร		1. ทำให้ธุรกรรมเกิดความล่าช้า 2. มีการดูแลที่ซับซ้อน 3. การมีส่วนร่วมของผู้ที่เกี่ยวข้องไม่น่าเชื่อถือ 4. ศักยภาพในการตรวจสอบ (Miner) 5. ต้องมีสิ่งจูงใจเพื่อรักษาเครือข่าย

ที่มา : สำนักงานพัฒนารัฐบาลดิจิทัล (2564)

โดยสรุป โครงข่ายบล็อกเชนแบ่งออกเป็น 3 ประเภท คือ (1) บล็อกเชนสาธารณะ อนุญาตให้ทุกคนเข้าร่วมและมีการกระจายอำนาจอย่างสมบูรณ์ (2) บล็อกเชนส่วนตัว ซึ่งอาจเรียกได้ว่าเป็นบล็อกเชนที่มีการจัดการ เป็นบล็อกเชนที่ได้รับอนุญาตซึ่งควบคุมโดยองค์กรเดียว ในบล็อกเชนส่วนตัวผู้มีอำนาจส่วนกลางจะกำหนดว่าใครสามารถเป็นโหนดได้ และ (3) บล็อกเชนเฉพาะกลุ่ม (Consortium Blockchain) ที่ผสมผสานการทำงานของบล็อกเชนสาธารณะกับบล็อกเชนส่วนตัว

13 Permissionless Blockchain หมายถึงบล็อกเชนที่เปิดให้ทุกคนมีสิทธิ์ในการเข้าถึงเครือข่ายและข้อมูลได้อย่างอิสระ โดยไม่จำเป็นต้องขออนุญาต ทั้งนี้อาจเรียกอีกชื่อหนึ่งว่า Public Blockchain

1.6 ประโยชน์และข้อเสียของบล็อกเชน

ประโยชน์และข้อเสียของบล็อกเชน มีดังนี้

1.6.1 ประโยชน์ของบล็อกเชน

บล็อกเชนมีประโยชน์ดังนี้ (Yen & Wang, 2021)

1. สามารถรองรับการทำธุรกรรมที่ซ้ำ ๆ ได้ดี โดยการดำเนินการมักจะสิ้นเปลืองพลังงานไปกับการเก็บบันทึกที่ซ้ำกัน และการตรวจสอบจากบุคคลที่สาม ระบบการเก็บบันทึกอาจเสี่ยงต่อการฉ้อโกงและการโจมตีทางไซเบอร์ ซึ่งความโปร่งใสที่จำกัดอาจทำให้การตรวจสอบข้อมูลช้าลง และด้วยการมาถึงของอินเทอร์เน็ตเพื่อสรรพสิ่ง (Internet of Things; IoT) ปริมาณธุรกรรมก็พุ่งสูง ทั้งหมดนี้ทำให้ธุรกิจช้าลง เสียกำไร และหมายความว่าต้องการวิธีที่ดีกว่า จึงเข้าสู่ยุคบล็อกเชน

2. ความไว้วางใจที่มากขึ้น ด้วยบล็อกเชนในฐานะสมาชิกของเครือข่ายเฉพาะสมาชิกสามารถมั่นใจได้ว่าจะได้รับข้อมูลที่ถูกต้องและรวดเร็ว รวมถึงบันทึกบล็อกเชนที่เป็นความลับจะถูกแชร์กับสมาชิกเครือข่ายที่ให้สิทธิ์การเข้าถึงโดยเฉพาะเท่านั้น

3. ความปลอดภัยที่มากขึ้น สมาชิกเครือข่ายทุกคนจำเป็นต้องมีฉันทามติเกี่ยวกับความถูกต้องของข้อมูล และธุรกรรมที่ตรวจสอบแล้วทั้งหมดจะไม่เปลี่ยนแปลงเนื่องจากจะถูกบันทึกอย่างถาวร ไม่มีผู้ใดแม้แต่ผู้ดูแลระบบที่สามารถลบธุรกรรมได้

4. ประสิทธิภาพมากขึ้น ด้วยบัญชีแยกประเภทที่ใช้ร่วมกันระหว่างสมาชิกของเครือข่าย การกระทบยอดบันทึกที่เสียเวลาจะถูกตัดออก และเพื่อเพิ่มความเร็วในการทำธุรกรรม สามารถจัดเก็บชุดกฎที่เรียกว่า สมาร์ตคอนแทรกต์บนบล็อกเชนและดำเนินการโดยอัตโนมัติ

1.6.2 ข้อเสียของธุรกรรมแบบเดิม

ในระบบธุรกรรมปัจจุบันซึ่งใช้เงินสดจะพบว่า เงินสดสามารถใช้ได้เฉพาะในการทำธุรกรรมจำนวนน้อยในพื้นที่เท่านั้น รวมทั้งใช้เวลารอมากในการประมวลผลธุรกรรม เนื่องจากต้องการบุคคลที่สามในการตรวจสอบและดำเนินการธุรกรรมทำให้กระบวนการซับซ้อน นอกจากนี้หากเครื่องเซิร์ฟเวอร์ (Central Server) เช่น เซิร์ฟเวอร์ของธนาคารถูกบุกรุก ทั้งระบบจะได้รับผลกระทบรวมถึงผู้เข้าร่วมด้วย ในขณะเดียวกันองค์กรที่ตรวจสอบต่างคิดค่าบริการสูง จึงทำให้กระบวนการมีราคาแพงในการทำธุรกรรมในแบบเดิม (Gupta, 2019)

ซึ่งการพัฒนาเทคโนโลยีบล็อกเชนขึ้นมา ช่วยสร้างความไว้วางใจและความโปร่งใสในการทำธุรกรรมซึ่งมีคุณสมบัติ 5 ประการต่อไปนี้

1. คุณสมบัติด้านการกระจาย (Distributed) บัญชีแยกประเภทมีการแบ่งปันและอัปเดตกับทุกธุรกรรมที่เข้ามาระหว่างโหนดที่เชื่อมต่อกับบล็อกเชนทั้งหมดนี้ดำเนินการแบบเรียลไทม์ เนื่องจากไม่มีเซิร์ฟเวอร์กลาง (Server) ที่ควบคุมข้อมูล

2. คุณสมบัติด้านความปลอดภัย (Secure) ไม่มีการเข้าถึงบล็อกเชนโดยไม่ได้รับอนุญาตผ่านการอนุญาตและการเข้ารหัส

3. คุณสมบัติด้านความโปร่งใส (Transparent) เนื่องจากทุกโหนดหรือผู้เข้าร่วมในบล็อกเชนมีสำเนาของข้อมูลบล็อกเชน ผู้ใช้สามารถเข้าถึงข้อมูลธุรกรรมทั้งหมดได้ โดยสามารถยืนยันตัวตนได้โดยไม่ต้องใช้คนกลาง

4. การดำเนินตามฉันทามติ (Consensus–based) ผู้เข้าร่วมเครือข่ายที่เกี่ยวข้องทั้งหมดต้องยอมรับว่าธุรกรรมนั้นถูกต้อง สิ่งนี้ทำได้โดยการใช้อัลกอริทึมฉันทามติ (Consensus Algorithms)

5. มีความยืดหยุ่น (Flexible) สัญญาอัจฉริยะหรือสมาร์ตคอนแทรกต์ที่ดำเนินการตามเงื่อนไขบางประการสามารถเขียนลงในแพลตฟอร์มได้ ซึ่งเครือข่ายบล็อกเชนสามารถพัฒนาไปพร้อมกับกระบวนการทางธุรกิจ

บล็อกเชนมีทั้งข้อดีและสามารถปรับข้อเสียของการทำงานธุรกรรมแบบเดิมให้สามารถรองรับการทำธุรกรรมที่ซ้ำ ๆ ได้ ทำให้การทำธุรกรรมสามารถสร้างความไว้วางใจและมีความปลอดภัยจากการโจมตีและมีประสิทธิภาพที่มากขึ้น

1.7 แนวทางการประยุกต์ใช้บล็อกเชน

แนวทางการประยุกต์ใช้บล็อกเชน มีดังนี้

1.7.1 แนวทางการประยุกต์ใช้เทคโนโลยีบล็อกเชน

ในปัจจุบันเทคโนโลยีบล็อกเชนอยู่ในช่วงของการเริ่มต้นนำไปใช้งานกับทุกอุตสาหกรรมและทุกภาคส่วนทั่วโลก ซึ่งมูลค่ารวมของธุรกรรมที่มีการใช้งานบนเทคโนโลยีบล็อกเชน รวมถึงบิตคอยน์นั้นยังมีปริมาณค่อนข้างน้อยเมื่อเทียบกับ GDP ของโลก ซึ่งมีเพียง 0.025% หรือ 12,000 ล้านดอลลาร์สหรัฐฯ ซึ่งจากรายงานของ World Economic Forum Survey (2015) พบว่าการใช้งานเทคโนโลยีบล็อกเชนมีแนวโน้มที่จะเป็นไปอย่างก้าวกระโดดภายใน 10 ปี เนื่องจากภาคอุตสาหกรรมและธุรกิจต่าง ๆ ตระหนักถึงประโยชน์และความสำคัญของการนำเทคโนโลยีบล็อกเชนไปใช้งาน ซึ่งเติบโตเพิ่มมากขึ้นถึง 60% การประยุกต์ใช้เทคโนโลยีบล็อกเชนได้ถูกนำมาใช้กันอย่างกว้างขวางเพื่อทำให้เกิดประสิทธิภาพในการปฏิบัติงานเพิ่มมากยิ่งขึ้น (ดังแสดงในรูปที่ 1.17)

1. การโอนเงิน แนวคิดดั้งเดิมที่อยู่เบื้องหลังการประดิษฐ์เทคโนโลยีบล็อกเชนยังคงเป็นแอปพลิเคชันที่ยอดเยี่ยม การโอนเงินโดยใช้บล็อกเชนอาจมีราคาถูกกว่าและเร็วกว่าการใช้บริการโอนเงินที่มีอยู่ โดยเฉพาะอย่างยิ่งสำหรับธุรกรรมข้ามพรมแดน ซึ่งมักจะช้าและมีราคาแพง แม้แต่ในระบบการเงินสมัยใหม่ การโอนเงินระหว่างบัญชีอาจใช้เวลาหลายวัน ในขณะที่ธุรกรรมบล็อกเชนใช้เวลาเพียงไม่กี่นาที

รูปที่ 1.18 การประยุกต์ใช้บล็อกเชน
ที่มา : ประยุกต์จากสำนักงานพัฒนาดิจิทัล (2564)

2. การแลกเปลี่ยนทางการเงิน หลายบริษัทได้ปรากฏขึ้นในช่วงไม่กี่ปีที่ผ่านมาโดยเสนอการแลกเปลี่ยนสกุลเงินดิจิทัลแบบกระจายอำนาจ ซึ่งการใช้บล็อกเชนสำหรับการแลกเปลี่ยนช่วยให้การทำธุรกรรมดำเนินการได้เร็วและราคาไม่แพง นอกจากนี้การแลกเปลี่ยนแบบกระจายอำนาจไม่ต้องการให้นักลงทุนฝากสินทรัพย์ของตนกับอำนาจจากส่วนกลาง ซึ่งหมายความว่าผู้ใช้ระบบรักษาการควบคุมและมีความปลอดภัยที่มากขึ้น ในขณะที่การแลกเปลี่ยนบนบล็อกเชนนั้นเกี่ยวข้องกับคริปโทเคอร์เรนซีเป็นหลัก แต่แนวคิดนี้สามารถนำไปใช้กับการลงทุนแบบเดิม ๆ ได้เช่นกัน

3. การให้ยืม ผู้ให้กู้สามารถใช้บล็อกเชนเพื่อดำเนินการสินเชื่อที่มีหลักประกันผ่านสัญญาอัจฉริยะ (Intelligent Signal) ที่สร้างขึ้นบนบล็อกเชนช่วยให้เหตุการณ์บางอย่างสามารถกระตุ้นสิ่งต่าง ๆ ได้โดยอัตโนมัติ เช่น การชำระค่าบริการ การเรียกหลักประกัน การชำระคืนเงินกู้เต็มจำนวน และการปล่อยหลักประกัน เป็นผลให้การประมวลผลเงินกู้เร็วขึ้นและราคาไม่แพง และผู้ให้กู้สามารถเสนออัตราที่ดีกว่า

4. ประกันภัย การใช้สมาร์ตคอนแทรกต์บนบล็อกเชนทำให้เกิดความโปร่งใสมากขึ้นสำหรับลูกค้าและผู้ให้บริการประกันภัย โดยการบันทึกการอ้างสิทธิ์ทั้งหมดบนบล็อกเชนจะป้องกันไม่ให้ลูกค้าอ้างสิทธิ์ซ้ำสำหรับเหตุการณ์เดียวกัน นอกจากนี้การใช้สมาร์ตคอนแทรกต์สามารถเร่งกระบวนการให้ผู้อ้างสิทธิ์ได้รับการชำระเงินได้

5. อสังหาริมทรัพย์ การทำธุรกรรมด้านอสังหาริมทรัพย์ต้องใช้เอกสารจำนวนมากในการตรวจสอบข้อมูลทางการเงินและความเป็นเจ้าของ จากนั้นจึงโอนโฉนดและกรรมสิทธิ์ให้เจ้าของใหม่ การใช้เทคโนโลยีบล็อกเชนเพื่อบันทึกธุรกรรมด้านอสังหาริมทรัพย์ทำให้วิธีการตรวจสอบและโอนความเป็นเจ้าของที่ได้ปลอดภัยและเข้าถึงมากขึ้น สามารถเพิ่มความเร็วในการทำธุรกรรม ลดงานเอกสาร และประหยัดเงินสำหรับการดำเนินการ

6. รักษาความปลอดภัยข้อมูลส่วนบุคคล การเก็บรักษาข้อมูล เช่น หมายเลขประกันสังคม วันเกิด และข้อมูลระบุตัวตนอื่นๆ ในบัญชีแยกประเภทสาธารณะ (เช่น บล็อกเชน อาจมีความปลอดภัยมากกว่าระบบปัจจุบันที่เสี่ยงต่อการถูกแฮ็ก เทคโนโลยีบล็อกเชนสามารถใช้เพื่อรักษาความปลอดภัยในการเข้าถึงข้อมูลระบุตัวตน ในขณะเดียวกันสามารถปรับปรุงการเข้าถึงสำหรับผู้ที่ต้องการข้อมูลดังกล่าวในอุตสาหกรรมต่างๆ เช่น การเดินทาง การดูแลสุขภาพ การเงิน และการศึกษา

7. โหวต (Vote) หากข้อมูลประจำตัวส่วนบุคคลถูกเก็บไว้ในบล็อกเชนจะทำให้นำไปใช้เพื่อการลงคะแนนโดยใช้เทคโนโลยีบล็อกเชนเพียงขั้นตอนเดียว ซึ่งการใช้เทคโนโลยีบล็อกเชนทำให้แน่ใจได้ว่าไม่มีใครโหวตสองครั้ง และมีเพียงผู้มีสิทธิ์เลือกตั้งที่มีสิทธิ์เท่านั้นที่สามารถลงคะแนนได้ และไม่สามารถแก้ไขการโหวตได้ นอกจากนี้ยังสามารถเพิ่มการเข้าถึงการโหวตด้วยการทำให้ง่ายเพียงแค่กดปุ่มสองสามปุ่มบนสมาร์ตโฟน ในขณะเดียวกันค่าใช้จ่ายในการจัดการเลือกตั้งจะลดลงอย่างมาก

8. โครงการของรัฐบาล อีกวิธีหนึ่งในการใช้ข้อมูลประจำตัวดิจิทัลที่จัดเก็บไว้ในบล็อกเชนคือ การบริหารผลประโยชน์ของรัฐบาล เช่น โครงการสวัสดิการ ประกันสังคม และเมดิแคร์ การใช้เทคโนโลยีบล็อกเชนสามารถลดการฉ้อโกงและค่าใช้จ่ายในการดำเนินงานได้ ในขณะเดียวกันผู้รับผลประโยชน์สามารถรับเงินได้เร็วขึ้นผ่านการเบิกจ่ายทางดิจิทัลบนบล็อกเชน

9. แบ่งปันข้อมูลทางการแพทย์อย่างปลอดภัย การเก็บเวชระเบียนบนบล็อกเชนช่วยให้แพทย์และผู้เชี่ยวชาญทางการแพทย์ได้รับข้อมูลที่ถูกต้องและเป็นปัจจุบันเกี่ยวกับผู้ป่วย ที่สามารถมั่นใจได้ว่าผู้ป่วยที่ไปพบแพทย์หลายคนจะได้รับการดูแลที่ดีที่สุด นอกจากนี้ยังสามารถเร่งระบบการดึงเวชระเบียนเพื่อให้สามารถรักษาได้ทันท่วงทีในบางกรณี และหากข้อมูลการประกันถูกเก็บไว้ในฐานข้อมูล แพทย์จะสามารถตรวจสอบได้อย่างง่ายดายว่าผู้ป่วยมีประกันหรือไม่และรักษาได้ครอบคลุมสิทธิ์การรักษาของผู้ป่วย

10. ค่าลิขสิทธิ์ศิลปิน การใช้เทคโนโลยีบล็อกเชนในการติดตามไฟล์เพลงและภาพยนตร์ที่เผยแพร่ทางอินเทอร์เน็ต ทำให้แน่ใจได้ว่าศิลปินจะได้รับค่าตอบแทนผลงาน เนื่องจากเทคโนโลยีบล็อกเชนถูกคิดค้นขึ้นเพื่อให้แน่ใจว่าไม่มีไฟล์เดียวกันมากกว่าหนึ่งแห่ง จึงสามารถนำมาใช้เพื่อช่วยลดการละเมิดลิขสิทธิ์ได้ ยิ่งไปกว่านั้นการใช้บล็อกเชนเพื่อติดตามการเล่นบนบริการสตรีมมิงและสัญญาอัจฉริยะหรือสมาร์ตคอนแทรกต์ในการกระจายการชำระเงินสามารถให้ความโปร่งใสมากขึ้นและรับประกันว่าศิลปินจะได้รับเงินที่ค้างชำระจากค่าลิขสิทธิ์

11. โทเค็น (Token) ที่ไม่สามารถเปลี่ยนได้ โทเค็นที่ไม่สามารถเปลี่ยนได้หรือ NFT มักถูกมองว่าเป็นวิธีการเป็นเจ้าของสิทธิ์ในงานศิลปะดิจิทัล เนื่องจากบล็อกเชนป้องกันข้อมูลจากสองแห่ง ซึ่งการวาง NFT บนบล็อกเชนรับประกันว่ามีเพียงสำเนาของงานศิลปะดิจิทัลชิ้นเดียวที่มีอยู่ที่เปรียบเสมือนการลงทุนทางกายภาพ แต่ไม่มีข้อเสียของการจัดเก็บและการบำรุงรักษา NFT สามารถมีแอปพลิเคชันต่าง ๆ ได้ และท้ายที่สุดก็เป็นวิธีถ่ายทอดความเป็นเจ้าของทุกสิ่งที่สามารถแสดงด้วยข้อมูลได้นั่นเอง ซึ่งอาจเป็นโฉนดที่ดิน สิทธิ์ในการออกอากาศวิดีโอหรือตั๋วดิจิทัลงานต่าง ๆ

12. การติดตามการขนส่งและห่วงโซ่อุปทาน การใช้เทคโนโลยีบล็อกเชนเพื่อติดตามสิ่งของขณะเคลื่อนที่ผ่านเครือข่ายโลจิสติกส์หรือซัปพลายเชนมีข้อดีหลายประการคือ ประการแรกช่วยสื่อสารระหว่างคู่ค้าได้ง่ายขึ้น เนื่องจากมีข้อมูลอยู่ในบัญชีแยกประเภทสาธารณะที่ปลอดภัย ประการที่สอง ให้ความปลอดภัยและความสมบูรณ์ของข้อมูลมากขึ้น เนื่องจากข้อมูลบนบล็อกเชนไม่สามารถเปลี่ยนแปลงได้ นั่นหมายความว่าคู่ค้าด้านโลจิสติกส์และซัปพลายเชนสามารถทำงานร่วมกันได้ง่ายขึ้นด้วยความเชื่อใจมากขึ้น ซึ่งข้อมูลที่ให้มานั้นถูกต้องและเป็นปัจจุบัน

13. เครือข่ายอินเทอร์เน็ตเพื่อสรรพสิ่ง (Internet of Things; IoT) ที่ปลอดภัย IoT ทำให้ชีวิตคนในยุคปัจจุบันง่ายขึ้น แต่ก็เป็นการเปิดโอกาสให้ผู้กระทำความผิดเข้าถึงข้อมูลหรือเข้าควบคุมระบบที่สำคัญได้ง่ายขึ้น หากแต่เทคโนโลยีบล็อกเชนให้ความปลอดภัยมากขึ้นโดยการจัดเก็บรหัสผ่านและข้อมูลอื่น ๆ บนเครือข่ายแบบกระจายอำนาจแทนที่จะเป็นเซิร์ฟเวอร์แบบรวมศูนย์ นอกจากนี้ยังมีการป้องกันการปลอมแปลงข้อมูลเนื่องจากบล็อกเชนนั้นไม่สามารถเปลี่ยนแปลงได้ในทางปฏิบัติ

14. การจัดเก็บข้อมูล การเพิ่มเทคโนโลยีบล็อกเชนในโซลูชันการจัดเก็บข้อมูลสามารถให้ความปลอดภัยและความสมบูรณ์ยิ่งขึ้น เนื่องจากข้อมูลสามารถจัดเก็บในลักษณะการกระจายอำนาจได้ การที่จะแฮ็กและล้างข้อมูลทั้งหมดในเครือข่ายจึงทำได้ยาก ในขณะที่ผู้ให้บริการจัดเก็บข้อมูลแบบรวมศูนย์อาจมีจุดซ้ำซ้อนเพียงไม่กี่จุด นอกจากนี้ยังหมายถึงการเข้าถึงข้อมูลได้มากขึ้น เนื่องจากการเข้าถึงไม่จำเป็นต้องอาศัยการดำเนินงานของบริษัทเดียว ในบางกรณีการใช้บล็อกเชนสำหรับการจัดเก็บข้อมูลอาจมีราคาถูกกว่า

1.7.2 ความท้าทายในการประยุกต์ใช้เทคโนโลยีบล็อกเชน

แม้ว่าบล็อกเชนจะได้พยายามพิสูจน์ตัวเองว่าเป็นเทคโนโลยีของยุคใหม่ แต่อย่างไรก็ตาม ยังมีความกังวลของผู้ใช้ องค์กร และความท้าทายในบางประเด็นให้ศึกษาและพัฒนา กล่าวคือ

1. การคุ้มครองความเป็นส่วนตัวของผู้ใช้ (User Privacy Protection)

2. ความเร็วในการประมวลผล จำนวนกระบวนการต่อหน่วยเวลา (Processing Speed, Number of Processes Per unit of Time)

3. การทำรายการให้เสร็จสิ้น (Finalizing Transactions)

4. การประสานงานกับระบบที่มีอยู่ (Coordination with Existing Systems)

5. ความน่าเชื่อถือของบล็อกเชน (Blockchain Reliability)

6. ประเด็นเรื่องของกฎหมายที่คุ้มครอง

โดยสรุป การประยุกต์ใช้เทคโนโลยีบล็อกเชนได้ถูกนำมาใช้กันอย่างกว้างขวางทั่วโลก ไม่เพียงแต่ภาคการเงินและการธนาคารเท่านั้น หากแต่ได้ถูกนำไปประยุกต์ใช้ในทุกภาคส่วน เช่น ธุรกิจซัปพลายเชนและโลจิสติกส์ ธุรกิจประกันภัย สถาบันการศึกษา สถานพยาบาล อุตสาหกรรมการท่องเที่ยว ตลอดจนหน่วยงานภาครัฐเพื่อทำให้เกิดประสิทธิภาพในการปฏิบัติงานเพิ่มมากยิ่งขึ้น

1.8 กรณีศึกษาและงานวิจัยเกี่ยวกับเทคโนโลยีบล็อกเชน

เทคโนโลยีบล็อกเชนได้ถูกนำมาใช้ในหน่วยงานทั้งในภาครัฐและภาคเอกชนทั่วโลก โดยในหัวข้อนี้จะนำเสนอกรณีศึกษาในต่างประเทศและในประเทศ ซึ่งมีรายละเอียดดังนี้

1.8.1 กรณีศึกษาและงานวิจัยที่เกี่ยวกับการประยุกต์ใช้เทคโนโลยีบล็อกเชน ในต่างประเทศ

1. การพัฒนาระบบตรวจสอบเส้นทางการซื้อขายกัญชารัฐโคโลราโด ประเทศสหรัฐอเมริกา รัฐโคโลราโดแห่งประเทศสหรัฐอเมริกาได้ร่วมมือกับ The Institute of Cannabis Research at Colorado State University–Pueblo (Institute) ในการพัฒนาระบบตรวจสอบเส้นทางการซื้อขายกัญชารวมไปถึงผลิตภัณฑ์แปรรูปต่าง ๆ ในอุตสาหกรรมกัญชา (Industrial Hemp) ตั้งแต่ผู้ผลิตไปจนถึงผู้ซื้อและผู้ขาย โดยใช้เทคโนโลยีบล็อกเชนในการออกใบอนุญาตการดำเนินธุรกิจเกี่ยวกับกัญชา ทั้งนี้การซื้อขายกัญชาจะต้องเป็นการซื้อขายจากผู้ที่ได้รับใบอนุญาตในการดำเนินธุรกิจเกี่ยวกับกัญชาเท่านั้น ซึ่งการนำเทคโนโลยีบล็อกเชนมาใช้ในอุตสาหกรรมกัญชานั้นช่วยให้รัฐโคโลราโดสามารถบังคับใช้กฎหมาย และการจัดเก็บรายได้จากการทำอุตสาหกรรมกัญชาได้อย่างมีประสิทธิภาพยิ่งขึ้น รวมไปถึงช่วยตรวจสอบการกระทำความผิด อันเนื่องมาจากการซื้อขายกัญชาที่ผิดกฎหมายจากผู้ที่ไม่ได้รับอนุญาต นอกจากนี้

รัฐโคโลราโดได้มีการออกกฎหมายที่สำคัญว่าด้วยเรื่องการนำเทคโนโลยีบล็อกเชนมาใช้ในการตรวจสอบการกระทำความผิดเกี่ยวกับอุตสาหกรรมกัญชา รวมไปถึงผลิตภัณฑ์ต่าง ๆ ที่มีส่วนผสมของกัญชาตั้งแต่กระบวนการผลิตไปจนถึงกระบวนการซื้อขาย (สำนักงานพัฒนารัฐบาลดิจิทัล, 2564)

2. การพัฒนาบล็อกเชนผ่านแอปพลิเคชัน งานวิจัยของฮามิดและคณะ (Hameed et al., 2022) นำเสนอการบูรณาการเทคโนโลยีบล็อกเชนเข้ากับอุตสาหกรรมต่าง ๆ ผ่านแอปพลิเคชัน การออกแบบแอปพลิเคชัน ความปลอดภัย และด้านความเป็นส่วนตัว เพื่อแก้ปัญหาภัยคุกคามต่อผู้ใช้และข้อมูลของพวกเขา โดยการศึกษานี้นำเสนอการสำรวจที่ครอบคลุมและล้ำสมัยของแอปพลิเคชันอุตสาหกรรม 4.0 ที่ใช้บล็อกเชน โดยมุ่งเน้นที่การออกแบบแอปพลิเคชัน ความปลอดภัย และความเป็นส่วนตัว ข้อกำหนดตลอดจนการป้องกันการถูกโจมตีที่สอดคล้องกันบนระบบบล็อกเชนที่มีมาตรการรับมือที่อาจเกิดขึ้น นอกจากนี้ยังวิเคราะห์และจัดให้มีการจำแนกเทคนิคการรักษาความปลอดภัยและความเป็นส่วนตัวที่ใช้ในแอปพลิเคชันเหล่านี้ เพื่อปรับปรุงความก้าวหน้าของคุณสมบัติการรักษาความปลอดภัย นอกจากนี้ยังเน้นประเด็นเปิดบางประการของการบูรณาการเทคโนโลยีบล็อกเชนในแอปพลิเคชันอุตสาหกรรมที่ช่วยออกแบบแอปพลิเคชันบนบล็อกเชนที่ปลอดภัยรวมไปถึงทิศทางในอนาคตเป็นอย่างไร (Gad et al., 2022)

3. การทบทวนวรรณกรรมเกี่ยวกับบล็อกเชน งานวิจัยของแกดและคณะ (Gad et al., 2022) ได้นำเสนอการทบทวนบทความที่มีอิทธิพลมากที่สุดเกี่ยวกับบล็อกเชนที่เผยแพร่ตั้งแต่ปี พ.ศ. 2556 – พ.ศ. 2563 (ค.ศ. 2013–ค.ศ. 2020) และจัดทำดัชนีโดย Web of Science Core Collection TM (WoS) ฐานข้อมูลวรรณกรรมของโลก เพื่อนำเสนอภาพรวมโดยย่อของเทคโนโลยีบล็อกเชนผ่านเอกสารที่รวบรวมมาได้ โดยมีการวิเคราะห์ตามคำถามการวิจัยที่สำคัญ 7 ข้อจาก 10 บทความที่ทรงอิทธิพล สิ่งพิมพ์ประจำปีและแนวโน้มการอ้างอิง สถานที่ตีพิมพ์ที่ได้รับความนิยมที่สุด รวมถึงรายงานการวิจัยแหล่งเงินทุนที่ได้รับการสนับสนุนมากที่สุด เพื่ออธิบายสถานะที่เป็นอยู่ แนวโน้มที่เกิดขึ้นใหม่ และขอบเขตของบล็อกเชน เพื่อเป็นแนวทางพื้นฐานสำหรับนักวิจัยและผู้ปฏิบัติงานทั้งใหม่และมีประสบการณ์ ก่อนที่จะเริ่มการวิจัยโครงการบนบล็อกเชนในอนาคต

นอกจากนี้ยังมีการอภิปรายเกี่ยวกับแอปพลิเคชันบล็อกเชนในโดเมนที่หลากหลาย พร้อมกับกรณีการใช้งานที่หลากหลาย สุดท้ายคือ การนำเสนอข้อมูลเชิงลึกโดยสังเขปเกี่ยวกับความท้าทายแบบเปิดและความก้าวหน้าที่อาจเกิดขึ้นในอนาคตเกี่ยวกับบล็อกเชน เพื่อช่วยเหลือบุคคลที่สนใจในการสำรวจและออกแบบโซลูชันบล็อกเชนใหม่โดยคำนึงถึงความต้องการที่มีอยู่และความท้าทาย (Six et al., 2022)

สำหรับฝั่งของการออกแบบซอฟต์แวร์ในมุมมองของวิศวกรซอฟต์แวร์ (Six et al., 2022) ได้นำความรู้เชิงลึกเกี่ยวกับรูปแบบซอฟต์แวร์ที่ใช้กับเทคโนโลยีบล็อกเชน ผ่านการทบทวนวรรณกรรมอย่างเป็นระบบจำนวน 120 รูปแบบที่ไม่ซ้ำกันและเสนออนุกรมวิธานของรูปแบบหลายประเภท ซึ่งสร้างขึ้นจากคอลเลกชันรูปแบบที่แยกออกมา โดยจุดประสงค์ของการรวบรวมคอลเลกชันนี้คือ การทำแผนที่จำแนกและอธิบายรูปแบบที่มีอยู่ทั้งหมดทั่วทั้งวรรณกรรม เพื่อช่วยให้ผู้อ่านตัดสินใจได้อย่างเพียงพอเกี่ยวกับการเลือกรูปแบบบล็อกเชน การศึกษานี้ยังแสดงให้เห็นการใช้งานที่เป็นไปได้ของรูปแบบเหล่านั้นและระบุความสัมพันธ์ระหว่างรูปแบบบล็อกเชนและรูปแบบซอฟต์แวร์อื่นๆ ที่ไม่ใช่บล็อกเชน

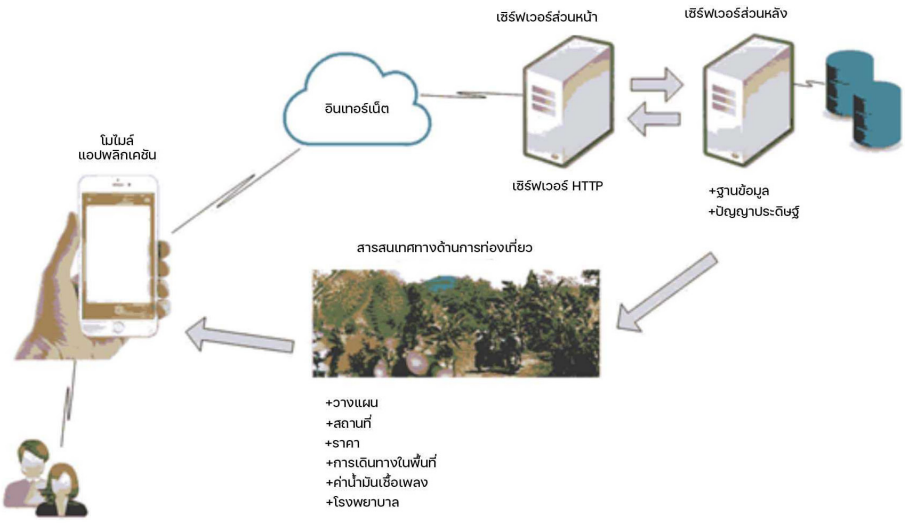
1.8.2 กรณีศึกษาและงานวิจัยที่เกี่ยวกับการประยุกต์ใช้เทคโนโลยีบล็อกเชนในประเทศไทย

1. การประยุกต์ใช้บล็อกเชนกับการท่องเที่ยว งานวิจัยของชางและคณะ (Chang et al., 2021) ได้ตระหนักถึงความก้าวหน้าทางเทคโนโลยีอินเทอร์เน็ตและอุตสาหกรรมเชิงนวัตกรรมที่ใช้ปัญญาประดิษฐ์จากบิ๊กดาต้าฐานข้อมูลขนาดใหญ่เป็นผู้นำอุตสาหกรรม 4.0 อย่างไรก็ตามโอกาสสำหรับสาธารณชนในการเรียนรู้เกี่ยวกับสกุลเงินดิจิทัลเสมือนหรือยูทิลิตีที่ใช้เทคโนโลยีบล็อกเชนนั้นมีจำกัด การศึกษานี้ตรวจสอบปัจจัยที่ส่งผลต่อการยอมรับเทคโนโลยีใหม่บนเกาะเชจู ประเทศเกาหลี ซึ่งธุรกิจการท่องเที่ยวเป็นธุรกิจหลัก กลุ่มตัวอย่างการศึกษาจำนวน 537 คนในเกาะเชจูและผู้ที่มาเยี่ยมชมจากแผ่นดินใหญ่ได้รับการวิเคราะห์โครงสร้างสี่เหลี่ยมจัตุรัสน้อยที่สุด (PLS) การสร้างแบบจำลองสมการ (SEM) และการออกแบบก่อนการทดสอบ–หลังการทดสอบกลุ่มเดียว ผ่านการสำรวจหลังจากชมคลิปวิดีโอเกี่ยวกับการใช้งานบล็อกเชนบนยูทูบ (YouTube) ผลการวิเคราะห์เชิงประจักษ์แสดงให้เห็นถึงผลกระทบของความโปร่งใสและความน่าเชื่อถือของบล็อกเชนที่มีต่อประสิทธิภาพและความคาดหวังของกลุ่มตัวอย่างการศึกษา พบว่าเงื่อนไขการอำนวยความสะดวกได้รับการยอมรับมากที่สุด โดยมีอิทธิพลในการยอมรับเทคโนโลยีบล็อกเชน หลังจากการทดลองใช้วิดีโอแนะนำการใช้งานบล็อกเชนเป็นสกุลเงินสำหรับการท่องเที่ยวเชจู การเปลี่ยนแปลงในเชิงบวกอย่างมีนัยสำคัญต่อการนำบล็อกเชนไปใช้ ซึ่งรายละเอียดในงานวิจัยนี้นำเสนอการประยุกต์ใช้เทคโนโลยีบล็อกเชนอย่างเป็นรูปธรรม และแสดงความเป็นไปได้ของการใช้โซเชียลมีเดีย เพื่อกระตุ้นการรับรู้ของผู้ใช้และความสนใจที่อาจเกิดขึ้นในตลาดการท่องเที่ยวภายในประเทศ

ซึ่งแนวทางการวิจัยนี้สามารถนำไปปรับใช้ได้กับงานวิจัยของผู้เขียนหนังสือเล่มนี้ (Suanpang et al., 2021) ที่มีจุดมุ่งหมายเพื่อพัฒนาการท่องเที่ยวเชิงเกษตรที่ใช้ปัญญาประดิษฐ์ (AI) เพื่อสนับสนุนการท่องเที่ยวโดยชุมชนในช่วงหลังโควิด–19 สำหรับมิติใหม่ของกรณีศึกษาแบบปกติถัดไป (Next Normal) โดยมีการประยุกต์ใช้ในจังหวัดศรีสะเกษ เพื่อมอบประสบการณ์ที่น่า

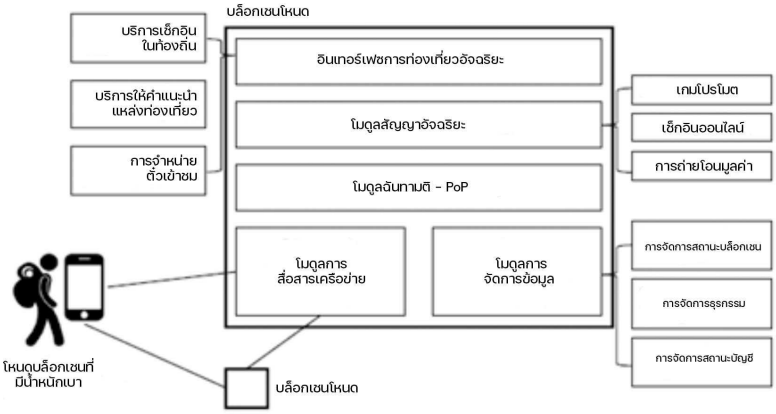
ประทับใจและรูปแบบใหม่ที่คำนึงถึงความต้องการของนักท่องเที่ยวในการท่องเที่ยวเชิงเกษตรในสวนทุเรียนภูเขาไฟ ในการวิจัยครั้งนี้ได้มีการพัฒนาระบบสนับสนุนการตัดสินใจและให้ข้อมูลการท่องเที่ยวผ่านแอปพลิเคชันมือถือเพื่อรวบรวมข้อมูลของผู้เดินทาง เช่น เพศ อายุ จำนวน วันที่เดินทาง งบประมาณ และรูปแบบการเดินทางที่ต้องการ ข้อมูลถูกส่งไปยังการจัดประเภทเพื่อสร้างโปรแกรมการท่องเที่ยวที่เหมาะสมโดยใช้ Extreme Learning Machine หลังจากขั้นตอนการจำแนกประเภทแล้ว กำหนดการเดินทางที่เหมาะสมจะถูกสร้างขึ้นและส่งกลับไปยังนักท่องเที่ยว นอกจากนี้ระบบที่เสนอยังมีส่วนข้อเสนอแนะและการให้คะแนนเพื่อประเมินความสอดคล้องของการจัดทัวร์ด้วยความพึงพอใจของผู้เดินทางในระดับสูง ในการประเมินระบบที่เสนอ ได้ทำการทดสอบข้อมูลจากนักท่องเที่ยว 400 คน (ดังแสดงในรูปที่ 1.19)

ผลการทดลองพบว่า นักท่องเที่ยวมีความพึงพอใจสูงสุด ด้วยกระบวนการที่รวดเร็ว สะดวก ระบบใช้งานง่าย และระบบมีความชัดเจน สวยงามตามลำดับ นอกจากนี้ AI ที่แนะนำการท่องเที่ยวเชิงเกษตรจะถูกนำมาใช้เพื่อสนับสนุนและส่งเสริมการท่องเที่ยวเชิงชุมชนในโครงการนำร่องในจังหวัดศรีสะเกษของประเทศไทย เพื่อส่งเสริมอุตสาหกรรมการท่องเที่ยวในช่วงหลังโควิด–19 เพื่อให้ได้แนวทางใหม่ของการเดินทางปกติถัดไป โดยในการพัฒนาในอนาคต ผู้วิจัยสามารถสอดแทรกการยอมรับการใช้บล็อกเชน และคริปโทเคอร์เรนซี ในการท่องเที่ยวภายในประเทศไทยในอนาคตได้ ทั้งนี้เพื่อให้นักท่องเที่ยวจากต่างประเทศได้รับความเป็นส่วนตัว การรักษาความปลอดภัยของข้อมูล รวมถึงการชำระค่าบริการและสินค้าระหว่างที่ท่องเที่ยวภายในประเทศไทยได้



รูปที่ 1.19 แสดง Theoretical Framework ของงานวิจัย AI Recommended Agrotourism Supporting Community–based Tourism Post COVID–19
ที่มา : Suanpang et al. (2021)

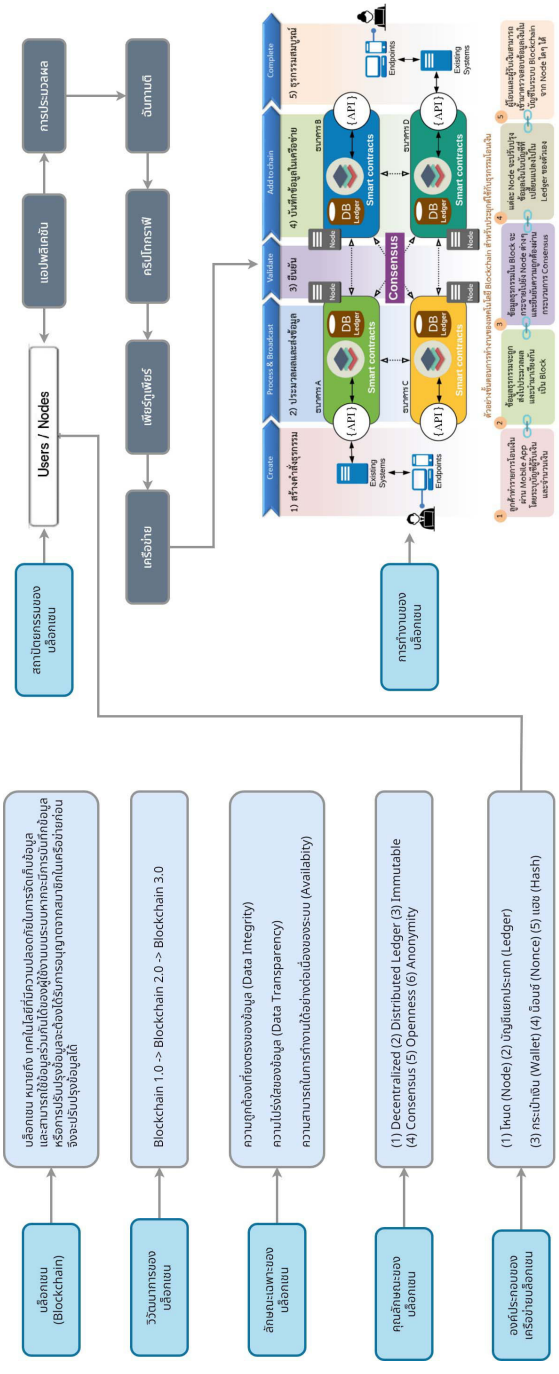
ในขณะที่งานวิจัยของหลัวและคณะ (Luo et al., 2021) ได้กล่าวถึงความต้องการเทคโนโลยีดิจิทัลอย่างเร่งด่วนของอุตสาหกรรมการท่องเที่ยวแบบดั้งเดิมเพื่อลดต้นทุนและเพิ่มประสิทธิภาพ โดยบล็อกเชนเป็นเทคโนโลยีเกิดขึ้นใหม่ที่มีแนวโน้มจะช่วยปฏิรูปอุตสาหกรรมการท่องเที่ยวเพราะเป็นแพลตฟอร์มที่น่าเชื่อถือในการเชื่อมโยงบริษัทท่องเที่ยวและนักท่องเที่ยว อย่างไรก็ตาม โซลูชันการท่องเที่ยวอัจฉริยะบนบล็อกเชนที่มีอยู่นั้นมีทั้งแนวคิดหรือข้อจำกัดในการแก้ปัญหาความท้าทายด้านการท่องเที่ยวขั้นพื้นฐาน ซึ่งในงานวิจัยนี้ได้นำเสนอบล็อกทัวร์ (BlockTour) ซึ่งเป็นแพลตฟอร์มการท่องเที่ยวอัจฉริยะบนบล็อกเชนพร้อมโซลูชันเฉพาะเพื่อจัดการกับความท้าทายและการปรับใช้ต้นแบบในโลกแห่งความเป็นจริง โดยเฉพาะอย่างยิ่ง ผู้วิจัยได้ออกแบบสถาปัตยกรรมระบบโดยรวมของบล็อกทัวร์ เพื่อเชื่อมโยงนักท่องเที่ยวและสถานที่ท่องเที่ยวด้วยวิธีที่น่าเชื่อถือ นอกจากนี้กลไกฉันทามติที่มีประสิทธิภาพยังได้รับการออกแบบด้วยแรงจูงใจให้นักท่องเที่ยวได้สำรวจสถานที่ท่องเที่ยวเพิ่มเติม สุดท้ายการใช้บล็อกทัวร์ และทำการทดลองเพื่อประเมินประสิทธิภาพ ผลการทดลองระบุว่าบล็อกทัวร์เป็นแพลตฟอร์มการท่องเที่ยวอัจฉริยะที่ใช้งานได้จริงและมีประสิทธิภาพสูง ทั้งนี้ แนวทางที่นำเสนอในบทความของหลัวและคณะ (Luo et al., 2021) สามารถนำไปต่อยอดในงานวิจัย AI recommended Agrotourism Supporting Community–based Tourism Post COVID–19 ของพรรณี สวนเพลง และคณะ (Suanpang et al., 2021) ได้ โดยสามารถเพิ่มความน่าเชื่อถือในข้อมูลประกอบการท่องเที่ยวให้กับนักท่องเที่ยว



รูปที่ 1.20 แสดงสถาปัตยกรรมของบล็อกทัวร์ (BlockTour)
ที่มา : Luo et al. (2021)

โดยสรุปบล็อกเชนเป็นเทคโนโลยีใหม่ที่ได้เริ่มมีการพัฒนาและนำไปประยุกต์ใช้กันอย่างแพร่หลายในหลากหลายอุตสาหกรรม ไม่ว่าจะเป็นธุรกิจ การค้า การธนาคาร การท่องเที่ยว การแพทย์ และการขนส่ง เพื่อช่วยเพิ่มขีดความสามารถในการทำธุรกิจให้มีประสิทธิภาพ สร้างมูลค่าตลอดห่วงโซ่อุปทานได้อย่างเป็นรูปธรรม

1.9 สรุป



รูปที่ 1.21 สรุปองค์ความรู้บทที่ 1

ที่มา : ผู้เขียน

จากรูปที่ 1.21 สรุปองค์ความรู้จากบทที่ 1 ดังนี้

“บล็อกเชน (Blockchain)” เป็นนวัตกรรมทางด้านเทคโนโลยีสารสนเทศในยุคปัจจุบันที่เริ่มนำมาประยุกต์ใช้กันอย่างแพร่หลายทั่วโลก นิยามของบล็อกเชน (Blockchain Definition) หมายถึง เทคโนโลยีที่มีความปลอดภัยในการจัดเก็บข้อมูล และสามารถใช้ข้อมูลร่วมกันได้ของผู้ใช้งานบนระบบ หากจะมีการบันทึกข้อมูลหรือการปรับปรุงข้อมูลจะต้องได้รับการอนุญาตจากสมาชิกในเครือข่ายก่อนจึงจะปรับปรุงข้อมูลได้

วิวัฒนาการของบล็อกเชนเริ่มตั้งแต่การพัฒนาแอปพลิเคชันบล็อกเชน ซึ่งสามารถแบ่งออกเป็น 3 ช่วงใหญ่ ๆ ตามขั้นตอนของการพัฒนา ได้แก่ Blockchain 1.0, Blockchain 2.0 และปัจจุบันอยู่ในยุค Blockchain 3.0 ที่มีการใช้สมาร์ตคอนแทรกต์เพื่อสร้างกระบวนการแบบกระจายศูนย์ที่เป็นอิสระ จึงทำให้ Blockchain 3.0 สามารถขับเคลื่อนองค์กรดิจิทัลเต็มรูปแบบที่ไม่จำเป็นต้องมีพนักงานในการช่วยทำธุรกรรมเลยในอนาคต

คุณลักษณะพื้นฐานที่สำคัญของการทำงานของบล็อกเชน 3 ประการ คือ ความถูกต้องเที่ยงตรงของข้อมูล (Data Integrity) ความโปร่งใสของข้อมูล (Data Transparency) และความสามารถในการทำงานได้อย่างต่อเนื่องของระบบ (Availability) อีกทั้งบล็อกเชนมีลักษณะการทำงานและลักษณะเฉพาะเหมือนกับบิตคอยน์ ซึ่งลักษณะเฉพาะของบล็อกเชน ได้แก่ (1) Decentralized (2) Distributed Ledger (3) Immutable (4) Consensus (5) Openness และ (6) Anonymity

บล็อกเชนเป็นเทคโนโลยีการประมวลผล และจัดเก็บข้อมูลแบบกระจายศูนย์ Distributed Ledger Technology; DLT) เป็นรูปแบบการบันทึกข้อมูลที่ใช้หลักการคริปโทกราฟีร่วมกับกลไกฉันทามติ (Consensus) ทำให้ข้อมูลที่ถูกบันทึกไปแล้วสามารถเปลี่ยนแปลงหรือแก้ไขได้ยาก เพิ่มความถูกต้องเชื่อถือได้ โปร่งใส และสามารถปรับปรุงข้อมูลได้ โดยบล็อกเชนมีองค์ประกอบที่สำคัญ ได้แก่ (1) บล็อก (2) โซ่ (3) ฉันทามติ และ (4) ความถูกต้อง และส่วนประกอบของเครือข่ายบล็อกเชน ประกอบไปด้วย (1) โหนด (2) บัญชีแยกประเภท (3) กระเป๋าเงิน (4) น็อนซ์ และ (5) แฮช

สถาปัตยกรรมของบล็อกเชนมีการทำงานเป็นชั้นหรือเลเยอร์ มีลักษณะทำงานเป็นเลเยอร์ (Layer) ได้แก่ (1) เครือข่าย (Network) เป็นเลเยอร์ต่ำสุด เครือข่ายซึ่งมักจะเป็นอินเทอร์เน็ต และ ICP/IP ที่จะเป็นพื้นฐานและจัดเตรียมเลเยอร์การสื่อสารพื้นฐานสำหรับบล็อกเชน (2) P2P เครือข่ายเพียร์ทูเพียร์ทำงานบนเลเยอร์เครือข่ายซึ่งประกอบด้วยข้อมูลโพรโทคอลการแพร่กระจาย เช่น Routing Protocols และ Folding Protocols (3) คริปโทกราฟีเป็นเลเยอร์การเข้ารหัสซึ่งมีโพรโทคอลการเข้ารหัสที่สำคัญ สำหรับการรับรองความปลอดภัยของบล็อกเชน

ประกอบด้วยการเข้ารหัสกุญแจสาธารณะและส่วนประกอบที่เกี่ยวข้อง เช่น ลายเซ็นดิจิทัล และฟังก์ชันแฮชเข้ารหัส (4) กลไกฉันทามติ ประกอบด้วยเทคนิคต่างๆ เช่น SMR กลไกฉันทามติตามหลักฐาน (Proof–based Consensus Mechanism) หรือแบบดั้งเดิม (Traditional) จากการวิจัยระบบกระจายแบบดั้งเดิมมักใช้ฉันทามติที่ทนต่อข้อผิดพลาดของ Byzantine Fault–tolerant (5) การดำเนินการ ซึ่งสามารถประกอบด้วยเครื่องเสมือนบล็อกธุรกรรม (6) แอปพลิเคชัน ซึ่งประกอบด้วยสมาร์ตคอนแทรกต์แอปพลิเคชันแบบกระจายศูนย์ DAO และตัวแทนอิสระ (Autonomous Agents) ชั้นนี้ได้อย่างมีประสิทธิภาพ มีตัวแทนระดับผู้ใช้ที่หลากหลายและโปรแกรมที่ทำงานบนบล็อกเชนผู้ใช้โต้ตอบกับบล็อกเชนผ่านแอปพลิเคชันที่กระจายอำนาจ

การทำงานของบล็อกเชนเริ่มตั้งแต่การกำหนดธุรกรรม ส่งข้อมูลลงในบล็อก และทำการตรวจสอบ ส่งข้อมูลไปจัดเก็บลงในโหนด และเสร็จสิ้นกระบวนการ

โครงข่ายบล็อกเชนแบ่งออกเป็น 3 ประเภท คือ (1) บล็อกเชนสาธารณะ ไม่ได้รับอนุญาตตามธรรมชาติ อนุญาตให้ทุกคนเข้าร่วมและมีการกระจายอำนาจอย่างสมบูรณ์ (2) บล็อกเชนส่วนตัว ซึ่งอาจเรียกได้ว่าเป็นบล็อกเชนที่มีการจัดการ เป็นบล็อกเชนที่ได้รับอนุญาตซึ่งควบคุมโดยองค์กรเดียว ในบล็อกเชนส่วนตัวผู้มีอำนาจส่วนกลางจะกำหนดว่าใครสามารถเป็นโหนดได้ และ (3) บล็อกเชนเฉพาะกลุ่ม (Consortium Blockchain) ที่ผสมผสานการทำงานของบล็อกเชนสาธารณะกับบล็อกเชนส่วนตัว

บล็อกเชนมีทั้งข้อดีและสามารถปรับข้อเสียของการทำงานธุรกรรมแบบเดิมให้สามารถรองรับการทำธุรกรรมที่ซ้ำๆ ได้ ทำให้การทำธุรกรรมสามารถสร้างความไว้วางใจและมีความปลอดภัยจากการโจมตีและมีประสิทธิภาพที่มากขึ้น

การประยุกต์ใช้เทคโนโลยีบล็อกเชนได้ถูกนำมาใช้กันอย่างกว้างขวางทั่วโลก ไม่เพียงแต่ภาคการเงินและการธนาคารเท่านั้น หากแต่ได้ถูกนำไปประยุกต์ใช้ในทุกภาคส่วน เช่น ธุรกิจซัปพลายเชนและโลจิสติกส์ ธุรกิจประกันภัย สถาบันการศึกษา สถานพยาบาล อุตสาหกรรมการท่องเที่ยว ตลอดจนหน่วยงานภาครัฐเพื่อทำให้เกิดประสิทธิภาพในการปฏิบัติงานเพิ่มมากยิ่งขึ้น

การพัฒนา BLOCKCHAIN นวัตกรรมแห่งอนาคต เป็นหนังสือที่ "บุกเบิก" องค์ความรู้การพัฒนาระบบ BLOCKCHAIN เพื่อรองรับการทำธุรกรรมทางการเงินที่ปลอดภัย ทรงพลัง และรองรับโลก DECENTRALIZED DISRUPTION

ประวัติผู้เขียน

รองศาสตราจารย์ ดร. พรรณี สวนเพลง (อาจารย์ประจำคณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสวนดุสิต)

ประวัติการศึกษา

- Doctor of Technology in Science (DTech), University of Technology Sydney, Australia
- Master of Information Technology (MIS), Griffith University, Australia
- Bachelor of Information Technology (B. IT), Major Information Systems (IS), Griffith University, Australia

ผลงานเขียนหนังสือตำราวิชาการ

- *ระบบสารสนเทศเชิงกลยุทธ์*
- *เทคโนโลยีสารสนเทศและนวัตกรรมสำหรับการจัดการความรู้*
- *ปฏิบัติการวิจัยทางด้านเทคโนโลยีสารสนเทศ*
- *การวิจัยทางด้านเทคโนโลยีสารสนเทศ*
- *การวิเคราะห์และออกแบบระบบสารสนเทศ*
- *การบริหารโครงการทางด้านเทคโนโลยีสารสนเทศ*
- *การวางแผนกลยุทธ์เทคโนโลยี*
- *ระบบสารสนเทศเพื่อการบริหารธุรกิจระหว่างประเทศ*
- *คอมพิวเตอร์สำหรับบัณฑิตศึกษา*
- *เทคโนโลยีสารสนเทศเพื่อชีวิต*

ผลงานวิจัย (มากกว่า 100 โครงการ)

- นวัตกรรมระบบสารสนเทศ, ระบบสารสนเทศเชิงกลยุทธ์, ปัญญาประดิษฐ์
- เทคโนโลยีสารสนเทศสำหรับการท่องเที่ยว (IT for Tourism)
- การท่องเที่ยว (Creative Tourism, Gastronomy Tourism, Cultural Tourism)
- การจัดการความรู้

พัฒนพงษ์ โพธิปัสสา (อาจารย์ประจำคณะศิลปศาสตร์และวิทยาศาสตร์ มหาวิทยาลัยราชภัฏศรีสะเกษ)

ประวัติการศึกษา

- วิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
- บริหารธุรกิจบัณฑิต สาขาคอมพิวเตอร์ธุรกิจ มหาวิทยาลัยมหาสารคาม

สาขาวิชาการที่มีความชำนาญพิเศษ

- การประมวลผลภาพ (Image Processing)
- การหาค่าที่เหมาะสม (Optimization)
- ปัญญาประดิษฐ์ (Artificial Intelligence)
- อินเทอร์เน็ตของสรรพสิ่ง (Internet of Things)
- ระบบเครือข่าย (Computer Networks)

พิมพ์ด้วยหมึก Soy Ink ปลอดภัยต่อร่างกาย ไม่ทำลายสิ่งแวดล้อม

พร้อมจำหน่ายในรูปแบบ
- ☑ e-book (PDF)
- ☐ e-book (EPUB)
- ☐ audiobooks
- ☑ ปกอ่อน
- ☐ LARGE PRINT (ตัวอักษรขนาดใหญ่)

ISBN 978-606-08-5047-1

289 บาท

คู่มือเรียน - สอบ / อุดมศึกษา - เทคโนโลยีสารสนเทศ, บริหารธุรกิจ, ศิลปศาสตร์และวิทยาศาสตร์

www.se-ed.com
sbc.fans
SE-ED Publisher