



## AI X-Ray Analysis on Blockchain

ระบบวิเคราะห์ภาพเอกซเรย์ด้วยปัญญาประดิษฐ์บนบล็อกเชน

โดย

ชื่อ นายรวิพล มุ่งดี	รหัสนักศึกษา B6506469
ชื่อ นายณัฐภูมิ อุปมัย	รหัสนักศึกษา B6509712
ชื่อ นายสิทธิินนท์ วงศ์สุทธิรัตน์	รหัสนักศึกษา B6606244
ชื่อ นางสาวนภสร วาริชอสังการ	รหัสนักศึกษา B6614768

รายงานนี้เป็นส่วนหนึ่งของรายวิชา ENG23 3055 เทคโนโลยีบล็อกเชนเบื้องต้น

หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์

สำนักวิชาวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีสุรนารี

ประจำภาคการศึกษาที่ 2 ปีการศึกษา 2568

## 1. ทำไมถึงเลือกใช้ Blockchain ให้กับบริการหรือระบบนั้นๆ

การนำเทคโนโลยี Blockchain มาใช้แทน Database แบบ Centralized ทัวไปในการจัดเก็บผลวิเคราะห์ภาพถ่ายทางการแพทย์ (X-rays) ร่วมกับ AI มีเหตุผลสำคัญดังนี้:

- 1.1. **ความทนทานต่อการแก้ไข (Immutability):** ข้อมูลทางการแพทย์เป็นข้อมูลที่ละเอียดอ่อนและมีผลทางกฎหมาย การใช้ Blockchain ทำให้มั่นใจได้ว่าผลวินิจฉัยจาก AI และประวัติการรักษาที่ถูกรับบันทึกไปแล้ว จะไม่สามารถถูกแอบเปลี่ยนแปลงย้อนหลังได้ (Tamper-proof) หากมีการแก้ไข ค่า Hash จะเปลี่ยนและระบบจะตรวจจับได้ทันที
- 1.2. **ตรวจสอบย้อนกลับได้ (Auditability & Transparency):** ระบบสามารถระบุได้ชัดเจนว่าข้อมูลชุดนี้ถูกสร้างขึ้นเมื่อไหร่ โดยโรงพยาบาลใด และผ่านการวิเคราะห์จาก AI เวอร์ชันไหน รวมถึงสามารถตรวจสอบสิทธิ์การเข้าถึง (Access Log) ได้อย่างโปร่งใส
- 1.3. **การแชร์ข้อมูลแบบรักษาความเป็นส่วนตัว (Privacy-Preserving Data Sharing):** การใช้ Public/Private Key (Asymmetric Encryption) ช่วยให้สามารถแชร์ข้อมูลข้ามโรงพยาบาลได้ โดยที่เฉพาะแพทย์ผู้ได้รับอนุญาตเท่านั้นที่มีสิทธิ์ถอดรหัสข้อมูลมาได้ ตัดปัญหาเรื่องข้อมูลรั่วไหลในขณะส่งต่อ

## 2. อธิบายการทำงานรวมของระบบ

ระบบ AI X-Ray Analysis on Blockchain แบ่งการทำงานออกเป็นส่วนย่อย (Modules) ที่ทำงานประสานกัน ดังนี้:

### 2.1. AI Diagnosis Unit (AI Service):

- รับภาพ X-ray จากเครื่องสแกน
- ประมวลผลด้วยโมเดล Deep Learning (เช่น CNN) เพื่อวินิจฉัยโรค (เช่น ปอดบวม, วัณโรค)
- ส่งคืนผลลัพธ์ (Diagnosis Result) และค่าความมั่นใจ (Confidence Score)

### 2.2. Encryption & Identity (Wallet):

- แพทย์แต่ละคนมีกุญแจคู่ (Key Pair): Public Key (สำหรับระบุตัวตนและเข้ารหัส) และ Private Key (สำหรับถอดรหัสข้อมูล)
- เมื่อได้ผลวิเคราะห์ ระบบจะกำหนดสิทธิ์การเข้าถึง (Access Control List) โดยทำการเข้ารหัสกุญแจข้อมูลด้วย Public Key ของแพทย์ที่มีสิทธิ์เท่านั้น

### 2.3. Blockchain Core:

- ทำหน้าที่รวบรวมข้อมูล (ผล AI + Access List + IPFS Hash ของรูปภาพ)
- สร้าง Block ใหม่ โดยเชื่อมโยงกับ Block ก่อนหน้าด้วยค่า Hash
- กระจายข้อมูลไปยัง Node ต่างๆ (โรงพยาบาลพันธมิตร) เพื่อขอฉันทามติ (Consensus)

### 3. อธิบาย Consensus - ทำไมถึงเลือก Consensus ลักษณะนี้, ป้องกัน 51% Attack อย่างไร, Incentive ในระบบคืออะไร

#### 3.1. รูปแบบที่เลือกใช้: Proof of Reputation & Validity (PoRV)

เราไม่เลือกใช้ Proof of Work (PoW) แบบ Bitcoin เพราะสิ้นเปลืองพลังงานและเข้าไปสำหรับการแพทย์ แต่เลือกใช้ระบบที่อิงความน่าเชื่อถือ (Reputation) ของ Node (โรงพยาบาล/สถาบันวิจัย)

#### 3.2. ทำไมถึงเลือกแบบนี้?

- ความเร็ว: ไม่ต้องแก้สมการคณิตศาสตร์ที่ซับซ้อน ทำให้ยืนยันธุรกรรมได้เกือบจะทันที
- ความเหมาะสม: ผู้เข้าร่วมในระบบ (Nodes) เป็นหน่วยงานที่ระบุตัวตนได้ (Known Entities) ไม่ใช่ใครก็ได้ (Anonymous)

#### 3.3. การป้องกัน 51% Attack

- Identity-Based Weighted Voting: สิทธิการโหวตไม่ได้ขึ้นอยู่กับกำลังเครื่อง (Computational Power) แต่ขึ้นอยู่กับ Reputation Score
- High Cost of Malicious Behavior: หาก Node ใดพยายามโหวตรับข้อมูลเท็จหรือ Spam ระบบ จะถูกตรวจสอบเจอได้ง่าย (เพราะระบุตัวตนได้) และจะถูกลดคะแนน Reputation จนเหลือ 0 ซึ่งส่งผลให้ถูกตัดออกจากระบบ
- Slashing: บทลงโทษคือการถูก "แบน" จากเครือข่าย ทำให้โรงพยาบาลนั้นเสียชื่อเสียงและเสียสิทธิการใช้งานระบบ ซึ่งเป็นต้นทุนทางสังคมและธุรกิจที่สูงมากจนไม่คุ้มที่จะโกง

#### 3.4. Incentive (แรงจูงใจในระบบ)

ระบบนี้ไม่มีการแจก "เหรียญดิจิทัล" (No Cryptocurrency Reward) แต่ใช้ "Data & Model Access" เป็นรางวัล:

- Benefit: Node ที่เข้าร่วมเป็น Validator และช่วยเก็บข้อมูล จะได้รับสิทธิ (Token) ในการเข้าถึง Global Dataset (ชุดข้อมูลภาพ X-ray รวมจากทุกโรงพยาบาลในเครือข่าย)
- Goal: เพื่อนำข้อมูลมหาศาลนี้ไปใช้ Train AI ของโรงพยาบาลตัวเองให้ฉลาดขึ้น แม่นยำขึ้น

4. ผลการทำงานของตัวอย่างจาก Code โดยมี Block เชื่อมต่อกันอย่างน้อย 5 Block