รายงาน ระบบ Blockchain ที่ใช้ในการทำ E-certificate

จัดทำโดย

นาย พอพล อินทรีย์ 61070133

ที่มา

เนื่องจากการทำ Webapplication E-certificate จำเป็นต้องใช้ Blockchain เพื่อช่วยให้ระบบน่าเชื่อถือ มีการตวรจสอบได้

ผลการศึกษา

จากการศึกษาระบบ Blockchain ที่นำมาใช้ โดยนำมาจากรุ่นพี่ปริญญาเอกที่ทำการศึกษา ในส่วน Blockchain โดยรุ่นพี่ปริญญาเอกได้ทำฟังก์ชั่นมาเพื่อให้ง่ายต่อการใช้งาน โดยมี 3 ส่วนหลัก คือ ส่วน Issuing Credential, Select Partial และ verify Credential โดยจะอธิบายทีละส่วน

ส่วนแรก Issuing Credential

เป็นส่วนแรกที่นำไว้ใช้ในการเพิ่ม Certificate ลงใน Blockchain โดยเป็นการนำชื่อของ Certificate แสดงความสัมพันธ์ของ Certificate นั้นๆ

รายละเอียด Input

รูปแบบไฟล์เป็นไฟล์ .zip โดย จะไฟล์จะประกอบไปด้วย

- Association คือ ความสัมพันธ์ของ Certificate ในการ upload ครั้งนั้นๆ
- Credential คือ Certificate ทั้งหมดที่จะ upload ไปในระบบ
- Issue_conf.json คือ ไฟล์ ที่กำหนด Address ที่จะนำไปไว้ใน Blockchain และมี Private key
- Issuer.json คือ ไฟล์ที่กำหนดผู้ Issue ว่า upload จากที่ไหนจากใคร

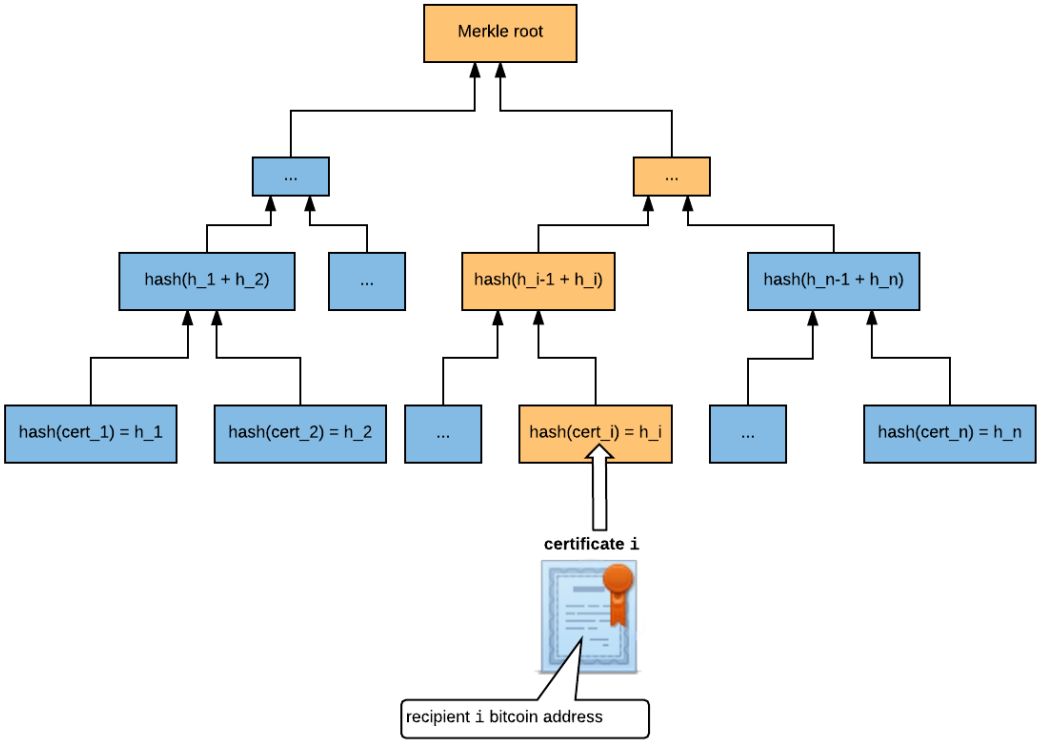
รายละเอียด output

- Credential คือ Certificate ทั้งหมดที่ upload ไปในระบบ

- Issuer.json คือ ไฟล์ที่กำหนดผู้ Issue ว่า upload จากที่ไหนจากใคร
- Manifest.json คือ ไฟล์ที่มี merkle tree ที่จะแสดงความสัมพันธ์ของ Credential ต่างๆ

หลักการทำงาน

จะนำcertificateทั้งหมดไปตรวจหาความสัมพันธ์ แล้วนำไปเข้ากระบวนการ hashing merkle tree ดั่งรูปภาพ



แล้วนำมาสร้าง manifest โดยนำ manifest นั้น upload address ไปยัง Blockchain

ส่วน Select Partial Credential

เป็นส่วน Verify เฉพาะบางส่วน คือ ตรวจสอบเฉพาะบาง Certificate

รายละเอียด Input

- Credential คือ Certificate ทั้งหมดที่จะ upload ไปในระบบ
- Issuer.json คือ ไฟล์ที่กำหนดผู้ Issue ว่า upload จากที่ไหนจากใคร
- Manifest.json คือ ไฟล์ที่มี merkle tree ที่จะแสดงความสัมพันธ์ของ Credential ต่างๆ

รายละเอียด output

สามารถดาวโหลด ข้อมูลที่ verify มาได้

- Credential คือ Certificate ทั้งหมดที่จะ upload ไปในระบบ
- Issuer.json คือ ไฟล์ที่กำหนดผู้ Issue ว่า upload จากที่ไหนจากใคร
- Manifest.json คือ ไฟล์ที่มี merkle tree ที่จะแสดงความสัมพันธ์ของ Credential ต่างๆ

หลักการทำงาน

จะตรวจสอบ Credential ทั้งหมด พร้อมกับ manifest ตรวจสอบใน Blockchain โดยตรวจเฉพาะที่เลือกให้ verify โดยการดาวโหลดใน manifest จะมี ค่าhashที่จำเป็นใช้เฉพาะกับ Credential นั้นๆ เพื่อนำไปตรวจสอบ

ส่วน Verify Credential

รายละเอียด input

- Credential คือ Certificate ทั้งหมดที่จะ upload ไปในระบบ
- Issuer.json คือ ไฟล์ที่กำหนดผู้ Issue ว่า upload จากที่ไหนจากใคร
- Manifest.json คือ ไฟล์ที่มี merkle tree ที่จะแสดงความสัมพันธ์ของ Credential ต่างๆ

รายละเอียด output

- จะแสดงCredentialนั้นถูกต้องหรือไม่ ถ้าถูกต้องจะแสดงข้อมูลความสัมพันธ์ของ Credential นั้นๆ

หลักการการทำงาน

จะนำ credential นั้นไป hash รวมกับค่า hash ใน manifest ไปตรวจสอบใน Blockchain โดยจะนำ Root ของ merkle tree ไปตรวจสอบตาม Address ที่อยู่ใน Blockchain