

โครงการวิศวกรรม
ภาควิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

เรื่อง

การประยุกต์ใช้สัญญาอัจฉริยะเพื่อควบคุมอุปกรณ์ไอโอทีบนเครือข่าย
บล็อกเชน

Implementation of Smart Contracts to Control IoT Device
on Blockchain Network

โดย

นาย ปาพจน์ บุษราคัม 6010501229
นาย วัชรพงษ์ จิตติประเสริฐ 6010501342

พ.ศ.2563

การประยุกต์ใช้สัญญาอัจฉริยะเพื่อควบคุมอุปกรณ์ไอโอทีบนเครือข่ายบล็อกเชน
Implementation of Smart Contracts to Control IoT Device on Blockchain Network

โดย

นาย ปาพจน์ บุษราคัม 6010501229
นาย วัชรพงษ์ จิตติประเสริฐ 6010501342

โครงการวิศวกรรม
ภาควิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

ตามหลักสูตร
วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้า

ได้รับการพิจารณาเห็นชอบโดย

อาจารย์ที่ปรึกษาโครงการ ทว:ภษ. วันที่ 19 เดือน เมษายน พ.ศ. 2564

(ผศ.ดร. ธีระภัทร จริยะนวิรัช)

กรรมการ ทว:ภษ. วันที่ 19 เดือน เม.ย. พ.ศ. 2564

(ผศ.ดร. ธนากร ช้องเดช)

นาย ปาพจน์ บุษราคัม 6010501229 ปีการศึกษา 2563

นาย วัชรพงษ์ จิตติประเสริฐ 6010501342 ปีการศึกษา 2563

การประยุกต์ใช้สัญญาอัจฉริยะเพื่อควบคุมอุปกรณ์ไอโอทีบนเครือข่ายบล็อกเชน

ปริญญาวิศวกรรมศาสตรบัณฑิต (สาขาวิชาวิศวกรรมไฟฟ้า) ภาควิชาวิศวกรรมไฟฟ้า

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

บทคัดย่อ

เนื่องด้วยในปัจจุบันเทคโนโลยีเครือข่ายบล็อกเชน (Blockchain) และเทคโนโลยีสัญญาอัจฉริยะ (Smart Contract) นั้นได้เป็นที่รู้จักกันแพร่หลายและถูกยอมรับกันในเรื่องของความปลอดภัยในระบบสามารถจัดการและป้องกันการโจรกรรมของข้อมูลได้พร้อมทั้งการเติบโตขึ้นของระบบเครือข่ายอินเทอร์เน็ตในทุกสิ่งที่มีการเชื่อมกันระหว่างเครือข่ายอินเทอร์เน็ตและอุปกรณ์ไฟฟ้าต่าง ๆ ทำให้มีการใช้งานที่หลากหลายและกำลังเป็นแนวทางใหม่ในการพัฒนาระบบอุตสาหกรรมมากมาย

ดังนั้นในโครงการนี้คณะผู้จัดทำจึงได้มีแนวคิดที่จะนำระบบเครือข่ายบล็อกเชนและเทคโนโลยีสัญญาอัจฉริยะมาใช้กับระบบไอโอทีซึ่งเกิดเป็นโครงการการประยุกต์ใช้สัญญาอัจฉริยะเพื่อควบคุมอุปกรณ์อินเทอร์เน็ตในทุกสิ่ง (Internet of Thing) บนเครือข่ายบล็อกเชนโดยจะดำเนินการพัฒนาและออกแบบสัญญาอัจฉริยะที่อยู่บนเครือข่ายบล็อกเชนมาเชื่อมต่อกับอุปกรณ์ไฟฟ้าที่เป็นระบบ IoT โดยเพื่อที่จะทำการควบคุมการทำงานของอุปกรณ์ได้โดยถูกต้องตามเงื่อนไขของการกำหนดในสัญญาอัจฉริยะ

หลังจากที่เชื่อมต่อกับระบบอินเทอร์เน็ตในทุกสิ่งแล้วจะสามารถควบคุมการทำงานของอุปกรณ์ไฟฟ้าได้ผ่านทางระบบเครือข่ายบล็อกเชนซึ่งเงื่อนไขการทำงานจะต้องอยู่ภายใต้สัญญาอัจฉริยะทำให้มีความสามารถในการจัดการความปลอดภัยและให้มีความน่าเชื่อถือมากขึ้นโดยหลังจากที่ระบบได้ถูกพัฒนาแล้วจะสามารถนำไปประยุกต์กับอุตสาหกรรมต่าง ๆ และเป็นแนวทางในการศึกษาต่อไปในภายภาคหน้า

คำสำคัญ เครือข่ายบล็อกเชน, สัญญาอัจฉริยะ, อินเทอร์เน็ตในทุกสิ่ง

เลขที่เอกสารอ้างอิงภาควิชา E5071-TRJ-2-2563

Paphot Busarakum Academic Year 2020

Vatcharapong Jittiprasert Academic Year 2020

Implementation of Smart Contracts to Control IoT Device on Blockchain Network

Bachelor Degree in Engineering Department Electrical

Faculty of Engineering, Kasetsart University

Abstract

As of nowadays, Blockchain technology and smart contract technology have become well known and accepted for system security, able to manage and prevent theft of information, as well as the growth of the internet of things. In everything there is an interconnection between the Internet and electrical equipment, it has a wide range of applications and is now a new way of developing many industrial systems.

Therefore, in this project, the organizers have the idea to apply Blockchain and smart contract technology to the internet of things, thus creating a smart contract application project to control the internet of things devices on Blockchain. It will develop and design smart contracts based on Blockchain to connect to IoT- based electrical devices. To control the operation of the equipment correctly according to the conditions of the smart contract

After being connected to the Internet of Things system, electrical equipment can be controlled via a Blockchain, where operating conditions are subject to smart contracts, enabling management, security and provide. Do more credibility after the system has been developed, it can be applied to various industries and as a guideline for further study in the future.

Keywords: Blockchain, Smart Contract, Internet of Things

Department Reference No E5071-TRJ-2-2563

กิตติกรรมประกาศ

ในการจัดทำโครงการนี้สำเร็จลุล่วงได้ด้วยความกรุณาจาก ผศ.ดร. ธีระภัทร จริยะนรวิษฐ์ อาจารย์ที่ปรึกษาโครงการ ที่ได้ให้คำแนะนำ แนวคิด ตลอดจนแก้ไขข้อบกพร่องต่าง ๆ เกี่ยวกับโครงการมาโดยตลอด คณะผู้ศึกษาจึงกราบขอบพระคุณเป็นอย่างสูง

คณะผู้จัดทำโครงการขอขอบคุณ อาจารย์คณะกรรมการ ผศ.ดร. ธนากร ษ์องค์เดช ที่ได้ให้ความกรุณาในการพิจารณา และให้ข้อคิด คำแนะนำในการจัดทำโครงการ

คณะผู้จัดทำโครงการ ขอขอบคุณ คณะวิศวกรรมศาสตร์ มหาวิทยาลัย เกษตรศาสตร์ ที่ได้ให้การสนับสนุนเป็นเงินทุนในการจัดทำโครงการนี้

คณะผู้จัดทำโครงการขอขอบพระคุณทุกท่านอย่างสูงที่ให้การสนับสนุน เอื้อเฟื้อและให้ความอนุเคราะห์ช่วยเหลือ จนกระทั่งโครงการนี้สำเร็จอย่างลุล่วงได้ด้วยดี

นาย ปาพจน์ บุษราคัม 6010501229

นาย วัชรพงษ์ จิตติประเสริฐ 6010501342

ผู้จัดทำ

สารบัญ

สารบัญ.....	VI
สารบัญภาพ.....	VII-VIII
คำอธิบายสัญลักษณ์และคำย่อ.....	IX
1 บทนำ.....	1
1.1. วัตถุประสงค์ของโครงการ.....	1
1.2. ขอบเขตของโครงการ.....	1
2 ทฤษฎีที่เกี่ยวข้อง.....	2
2.1. เทคโนโลยีบล็อกเชน.....	2
2.1.1. หลักการทำงานของเทคโนโลยีบล็อกเชน.....	3-4
2.1.2. คุณลักษณะพื้นฐานที่สำคัญของเทคโนโลยี บล็อกเชน.....	5
2.2. สัญญาอัจฉริยะ.....	6-7
2.3. อีเธอเรียม (Ethereum).....	8
2.4. ระบบอินเทอร์เน็ตในทุกสิ่ง.....	9
3 เครื่องมือที่ใช้ในการทำโครงการ.....	10
3.1. ฮาร์ดแวร์.....	10-11
3.2. ซอฟต์แวร์.....	12-14
4 วิธีการดำเนินโครงการ.....	15
4.1 กระบวนการรวบรวมข้อมูล.....	15
4.2 กระบวนการศึกษาข้อมูล.....	16-17
4.3 กระบวนการนำเสนอและจัดทำรูปเล่มรายงาน.....	18
5 ผลการดำเนินโครงการและวิจารณ์.....	19
5.1. ผลการออกแบบพัฒนาสัญญาอัจฉริยะ.....	20
5.1.1. องค์ประกอบของโค้ดสัญญาอัจฉริยะ.....	20-21
5.2. ผลการทดสอบการทำงานสัญญาอัจฉริยะ.....	22-23
5.3. ผลการนำสัญญาอัจฉริยะมาลงเว็บไซต์ที่สามารถเรียกใช้งานฟังก์ชันการทำงาน.....	23
5.3.1 ผลการนำสัญญาอัจฉริยะมา Deploy ลงใน MyEtherWallet.....	24

5.3.2.ผลการติดต่อสัญญาอัจฉริยะมาใน MyEtherWallet.....	25
5.4. ผลการเชื่อมต่อ สัญญาอัจฉริยะเข้ากับระบบไอโอที.....	26-27
6 สรุปผลการดำเนินงานและข้อเสนอแนะ.....	28
7 บรรณานุกรม	29
ประวัติனிสีต.....	30

สารบัญภาพ

รูปที่ 1 ระบบแบบ CENTRALIZED, DECENTRALIZED, DISTRIBUTED	2
รูปที่ 2 หลักการทำงานของเทคโนโลยี BLOCKCHAIN.....	7
รูปที่ 3 4 ขั้นตอนทำงานของเทคโนโลยี BLOCKCHAIN.....	4
รูปที่ 4 สัญลักษณ์ ETHEREUM.....	8
รูปที่ 5 ราสเบอร์รี่พาย	10
รูปที่ 6 มิเตอร์ไฟฟ้าอัจฉริยะ	11
รูปที่ 7 ระบบปฏิบัติการ Raspbian.....	12
รูปที่ 8 หน้าเว็บไซต์ REMIX-IDE	13
รูปที่ 9 LOGO METAMASK	13
รูปที่ 10 LOGO MYETHERWALLET.....	14
รูปที่ 11 แผนภาพขั้นตอนกระบวนการรวบรวมข้อมูล.....	15
รูปที่ 12 แผนภาพขั้นตอนกระบวนการศึกษาข้อมูล.....	17
รูปที่ 13 แผนภาพขั้นตอนกระบวนการนำเสนอ และจัดทำรูปเล่ม	18
รูปที่ 14 บัญชี METAMASK เลือกใช้ RINKEBY TEST NETWORK	19
รูปที่ 15 โค้ดของสัญญาอัจฉริยะส่วนของการประกาศตัวแปร.....	20
รูปที่ 16 โค้ดของสัญญาอัจฉริยะส่วนของการประกาศตัวแปร	21
รูปที่ 17 ค่า GAS ในการ DEPLOY สัญญาอัจฉริยะ	22
รูปที่ 18 การทดสอบ สัญญาอัจฉริยะใน REMIX-IDE.....	22
รูปที่ 19 รายละเอียดธุรกรรม ของการ Deploy สัญญาอัจฉริยะที่ตรวจสอบโดย ใช้รหัสที่อยู่ของสัญญา ในเว็บไซต์ ETHERSCAN.IO	23
รูปที่ 20 การเชื่อมต่อ MYETHERWALLET กับ METAMASK และข้อมูลบัญชี.....	23
รูปที่ 21 การนำสัญญาอัจฉริยะมา DEPLOY ลงใน MYETHERWALLET	24
รูปที่ 22 การติดต่อสัญญาอัจฉริยะมาใน MYETHERWALLET	25
รูปที่ 23 การเรียกฟังก์ชันและทดสอบการทำงาน สัญญาอัจฉริยะใน MYETHERWALLET	25
รูปที่ 24 ราสเบอร์รี่พายที่ต่อกับบอร์ดเพื่อควบคุมมิเตอร์อัจฉริยะ	26
รูปที่ 25 ราสเบอร์รี่พายที่ส่งรีเลย์จ่ายไฟเข้ามิเตอร์อัจฉริยะ.....	27
รูปที่ 26 ราสเบอร์รี่พายที่ส่งรีเลย์ตัดไฟมิเตอร์อัจฉริยะ	27

คำอธิบายสัญลักษณ์และคำย่อ

IoT	ย่อมาจาก Internet of Thing
ETH	ย่อมาจาก โทเคน สกุลเงินดิจิทัลของ Ethereum

1 บทนำ

ในปัจจุบันเทคโนโลยีบล็อกเชนได้มีการพัฒนาและเป็นที่ยอมรับมากขึ้น เนื่องด้วยเป็นเทคโนโลยีที่มีการกระจายศูนย์กลางการควบคุมและดำเนินการธุรกรรมในด้านต่างๆ ทำให้สามารถตรวจสอบธุรกรรมและความถูกต้องได้อย่างเท่าเทียมกันในระบบจึงทำให้เกิดความปลอดภัยสูงและสามารถป้องกันการโจรกรรมทางโลกอินเทอร์เน็ต ทำให้มีการนำไปประยุกต์ใช้มากขึ้นในหลายๆองค์กร รวมทั้งการเกิดขึ้นของเทคโนโลยีของสัญญาอัจฉริยะที่เกิดจากการเขียนโปรแกรมคอมพิวเตอร์ที่มีการระบุเงื่อนไขให้สัญญาอัจฉริยะมีผลต่อเมื่อมีเหตุการณ์ตามที่ระบุไว้เกิดขึ้นและเมื่อนำไปใช้ร่วมกับเครือข่ายบล็อกเชน ส่งผลในการเพิ่มศักยภาพเครือข่ายบล็อกเชนให้มีการดำเนินการที่เป็นอัตโนมัติและดำเนินการถูกต้องภายใต้เงื่อนไขที่กำหนดไว้ และสามารถตรวจสอบธุรกรรมได้อย่างโปร่งใส พร้อมทั้งการเติบโตขึ้นเทคโนโลยีอินเทอร์เน็ตในทุกสิ่งที่จะสามารถทำให้เกิดการอุปกรณ์ไฟฟ้าต่าง ๆ สามารถเชื่อมต่อและเข้าถึงได้เป็นโครงข่ายผ่านระบบอินเทอร์เน็ต

จากเหตุผลดังกล่าว โครงการฉบับนี้จึงได้ทำการศึกษาและพัฒนาาระบบสัญญาอัจฉริยะเพื่อนำไปสั่งการและควบคุมอุปกรณ์ IoT โดยเลือกใช้อุปกรณ์ไมโครคอนโทรลเลอร์ไฟฟ้าอัจฉริยะ ซึ่งระบบสัญญาอัจฉริยะจะทำงานผ่านระบบบล็อกเชนและควบคุมการทำงานของอุปกรณ์ไอโอทีให้ถูกต้องตามเงื่อนไขที่กำหนดไว้ในสัญญาอัจฉริยะ

1.1 วัตถุประสงค์ของโครงการ

ศึกษาและพัฒนาาระบบสัญญาอัจฉริยะเพื่อนำไปสั่งการและควบคุมอุปกรณ์ IoT โดยเลือกใช้อุปกรณ์ไมโครคอนโทรลเลอร์ไฟฟ้าอัจฉริยะ ซึ่งระบบสัญญาอัจฉริยะจะทำงานผ่านระบบบล็อกเชน

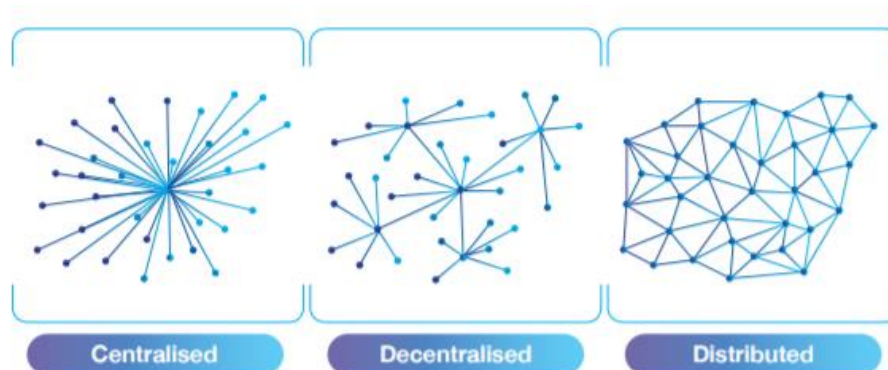
1.2 ขอบเขตของโครงการ

ศึกษาระบบเครือข่ายบล็อกเชนและระบบสัญญาอัจฉริยะ เพื่อที่จะทำการออกแบบและพัฒนาาระบบสำหรับการไปควบคุมสั่งการอุปกรณ์ IoT โดยเลือกใช้ Ethereum ซึ่งเป็นแพลตฟอร์มบล็อกเชนที่รองรับระบบสัญญาอัจฉริยะจากนั้นทำการศึกษาและอุปกรณ์ IoT เพื่อที่จะสามารถเชื่อมกับระบบเครือข่ายบล็อกเชน จากนั้นสามารถควบคุมสั่งการได้

2 ทฤษฎีที่เกี่ยวข้อง

2.1 เทคโนโลยีบล็อกเชน

บล็อกเชน คือเทคโนโลยีการจัดเก็บข้อมูลแบบ Shared Database หรือ ที่รู้จักกันในชื่อ “Distributed Ledger Technology (DLT)” โดยเป็นรูปแบบ การบันทึกข้อมูลที่รับประกันความปลอดภัยว่าข้อมูลที่ถูกบันทึกไปก่อนหน้านี้ ไม่สามารถที่จะเปลี่ยนแปลง หรือแก้ไขได้ ซึ่งทุกผู้ใช้งานจะได้เห็นข้อมูลชุดเดียวกัน ทั้งหมด โดยใช้หลักการ วิทยาการเข้ารหัสลับ (Cryptography) และความสามารถของ ระบบการประมวลผลแบบกระจาย (Distributed Computing) เพื่อสร้างกลไกความน่าเชื่อถือ (Yermack, 2017) จุดเริ่มต้นของเทคโนโลยี บล็อกเชน เกิดขึ้นครั้งแรกในปี 2008 โดยการนำเสนอของ “Satoshi Nakamoto” จากเอกสาร Bitcoin: A Peer-to-Peer Electronic Cash System เป็นการนำเสนอแนวคิดเกี่ยวกับการสร้าง แพลตฟอร์ม ที่สามารถสร้างความปลอดภัยในการแลกเปลี่ยนเงินสกุลดิจิทัลที่มีชื่อว่า “Bitcoin” โดยใช้ทฤษฎีเกี่ยวกับการทำ วิทยาการเข้ารหัสลับ และ ระบบการประมวลผลแบบกระจาย ซึ่งไม่จำเป็นต้องมีคนกลางเข้ามาเกี่ยวข้อง เช่น ธนาคาร หรือหน่วยงานอื่น ๆ ที่เกี่ยวข้องกับกระบวนการจ่ายเงิน โดยได้รับความสนใจอย่างแพร่หลาย รวมทั้ง ได้รับการยอมรับจากผู้เชี่ยวชาญทั่วโลกว่าเป็นเทคโนโลยีที่มีศักยภาพ และสามารถ นำมาประยุกต์ใช้ในภาคธุรกิจอื่น ๆ ได้ไม่เฉพาะแค่ภาคธุรกิจการเงินและการธนาคาร เท่านั้น แต่ยังรวมถึงภาครัฐก็ได้มีการตื่นตัวและศึกษาเกี่ยวกับเทคโนโลยี บล็อกเชน กันอย่างแพร่หลายเช่นกัน การทำงานของเทคโนโลยี บล็อกเชน อาศัยการจัดเก็บข้อมูลแบบกระจายศูนย์ (Distributed Ledger Technology) โดยทุกข้อมูลจะมีการเชื่อมโยงกันทั้งระบบ และเมื่อมีรายการธุรกรรมใหม่เกิดขึ้นจะต้องมีการประกาศบอกทุกเครื่องในระบบ ให้รับรู้

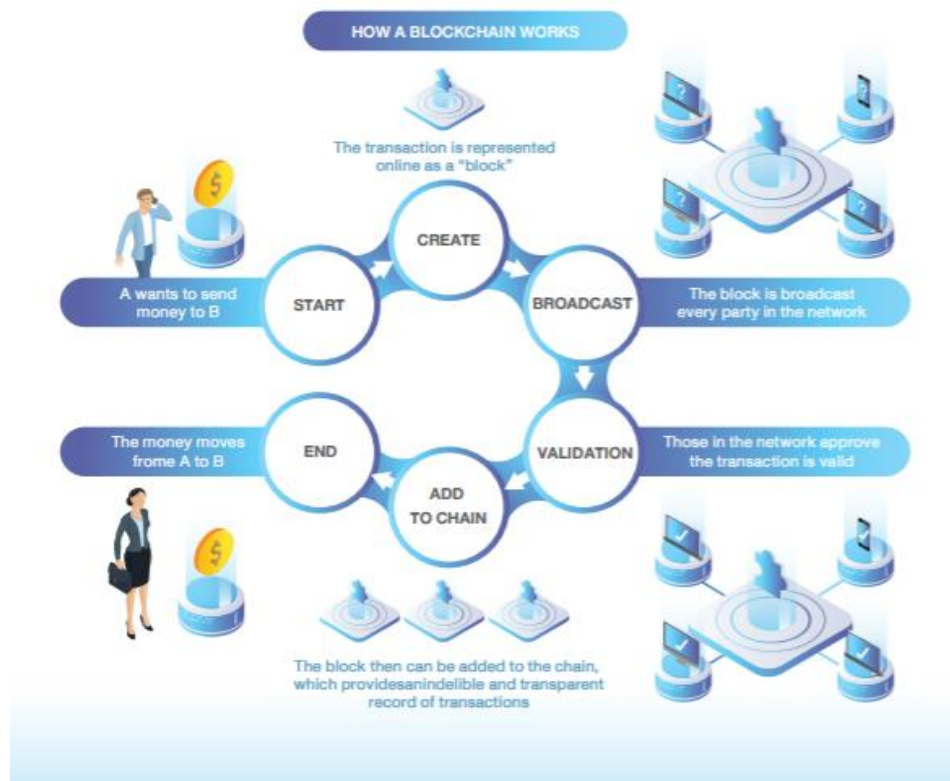


รูปที่1 ระบบแบบ Centralized, Decentralized, Distributed

ที่มา: https://www.dga.or.th/upload/download/file_ff487bacfb3198a615ca75112b8d156c.pdf

2.1.1 หลักการทำงานของเทคโนโลยีบล็อกเชน

หลักการทำงานของเทคโนโลยี บล็อกเชน คือ ฐานข้อมูลจะถูกแชร์ให้กับ ทุก โหนด 1 ที่อยู่เครือข่ายและการทำงานของเทคโนโลยี บล็อกเชนจะไม่มีเครื่องใดเครื่องหนึ่งเป็นศูนย์กลางหรือเครื่องแม่ข่าย ซึ่งการทำงานแบบกระจายศูนย์นี้ จะไม่ถูกควบคุมโดยคนเพียงคนเดียว แต่ทุก โหนด ที่อยู่เครือข่ายและการทำงานของเทคโนโลยีบล็อกเชน จะไม่มีเครื่องใดเครื่องหนึ่งเป็นศูนย์กลางหรือเครื่องแม่ข่าย ซึ่งการทำงานแบบกระจายศูนย์นี้ จะไม่ถูกควบคุมโดยคนเพียงคนเดียว แต่ทุก โหนด จะได้รับสำเนาฐานข้อมูลเก็บไว้ และจะมีการอัปเดตฐานข้อมูลแบบอัตโนมัติเมื่อมีข้อมูลใหม่เกิดขึ้น ทั้งนี้สำเนา ฐานข้อมูลของทุกคนในเครือข่ายจะต้องถูกต้อง และตรงกันกับของสมาชิกคนอื่นในเครือข่าย อีกทั้งการบันทึกข้อมูลเข้าสู่ บล็อก ยังอาศัยหลักการทำ วิทยาการเข้ารหัสลับ และการทำ Consensus2 จากสมาชิกในเครือข่ายด้วยกัน ก่อนทำการบรรจุข้อมูลลง



รูปที่2 หลักการทำงานของเทคโนโลยี Blockchain

ที่มา: https://www.dga.or.th/upload/download/file_ff487bacfb3198a615ca75112b8d156c.pdf

บล็อก และเพิ่มเข้าสู่ระบบ บล็อกเชน เพื่อเป็นการป้องกัน และรับประกันความ ปลอดภัยของข้อมูล โดยแต่ละ เครือข่าย บล็อกเชน จะมีการกำหนดกฎเกณฑ์ ในการตรวจสอบหรือที่เรียกว่า “Consensus Protocol” หรือ “Consensus Mechanism” ขึ้นมาเพื่อใช้ในเครือข่าย โดยหลักการทำงานพื้นฐานที่สำคัญ ของเทคโนโลยี บล็อกเชน อย่างน้อยจะต้องประกอบไปด้วย 4 ขั้นตอนหลัก ๆ ตามรูปภาพที่ 3



รูปที่3 4 ขั้นตอนทำงานของเทคโนโลยี Blockchain

ที่มา: https://www.dga.or.th/upload/download/file_ff487bacfb3198a615ca75112b8d156c.pdf

2.1.2 คุณลักษณะพื้นฐานที่สำคัญของเทคโนโลยี บล็อกเชน

การจัดเก็บข้อมูลในรูปแบบของ บล็อก โดยเชื่อมต่อแต่ละ บล็อก ด้วย ฟังก์ชันแฮช (Hash Function) และกระจายให้ทุก ๆ โหนด เก็บ ทำให้เกิดคุณสมบัติที่สำคัญของ บล็อกเชน 3 ประการ คือ ความถูกต้องเที่ยงตรงของข้อมูล (Data Integrity) ความโปร่งใสในการเข้าถึงข้อมูล (Data Transparency) และความสามารถในการทำงานได้อย่างต่อเนื่องของระบบ (Availability)

ความถูกต้องเที่ยงตรงของข้อมูล เนื่องจากการเชื่อมโยง บล็อก ปัจจุบันและ บล็อก ก่อนหน้าด้วย ฟังก์ชันแฮช และทำการกระจายให้ทุก โหนด เก็บ ทำให้ข้อมูลที่ถูกบันทึกลงใน บล็อกเชน แล้วไม่สามารถแก้ไข หรือเปลี่ยนแปลงข้อมูลได้ (Immutability) ดังนั้นหากมีความพยายามในการแก้ไขหรือเปลี่ยนแปลงข้อมูลที่ถูกบันทึกลงใน บล็อก แล้วจะทำให้ทราบได้ทันทีเนื่องจากข้อมูลใน โหนด ดังกล่าวจะมีข้อมูล ที่ต่างออกไปจาก โหนด อื่น ๆ ในระบบ และไม่สามารถสร้าง Consensus กับ โหนด อื่นได้ ทำให้ถูกแยกออกจาก Chain หลักไปในที่สุด

ความโปร่งใสในการเข้าถึงข้อมูล เนื่องจากทุก โหนด ในระบบ บล็อกเชน จะเก็บข้อมูลเดียวกันทั้งหมด โดยไม่มี โหนด ใด โหนด หนึ่งเป็นตัวกลางที่มีอำนาจแต่เพียงผู้เดียวในการ เก็บข้อมูล ดังนั้นการเข้าถึงข้อมูลใด ๆ จึงทำได้จาก โหนด ตัวเองทันที โดยไม่จำเป็นต้องร้องขอข้อมูลจากตัวกลาง จึงเรียกว่าเป็นระบบที่มีความ โปร่งใสในการเข้าถึงข้อมูลสูงมาก

ความสามารถในการทำงานได้อย่างต่อเนื่องของระบบ เนื่องจากทุก โหนด ในระบบ บล็อกเชน จะเก็บข้อมูลเดียวกันทั้งหมด จึงสามารถทำงานทดแทนกันได้เมื่อมี โหนด ที่ไม่สามารถให้บริการได้ในขณะนั้น โดยระบบจะทำการคัดลอกสำเนาข้อมูลให้เป็นข้อมูลชุดเดียวกันเมื่อ โหนด กลับขึ้นมาให้บริการได้อีกครั้ง

2.2 สัญญาอัจฉริยะ

สัญญาอัจฉริยะ คือ โปรแกรมคอมพิวเตอร์ที่สามารถดำเนินการตามข้อตกลง โดยอัตโนมัติทันทีที่เกิดเหตุการณ์ตามเงื่อนไขในสัญญาซึ่งได้มีการระบุถึง เงื่อนไข หรือเหตุการณ์ดังกล่าวไว้ล่วงหน้าแล้ว โดยไม่ต้องมีคนกลาง นั่นคือ หลักการสำคัญของสัญญาอัจฉริยะ ซึ่งได้ถูกคิดค้นขึ้นในปี 1994 โดย Nick Szabo (Crosby, Pattanayak, Verma, & Kalyanaraman, 2016) ยกตัวอย่างเช่น การโอนเงินจ่ายค่าลิขสิทธิ์ซอฟต์แวร์อัตโนมัติ ทันทีที่จำนวนผู้ใช้ถึงระดับที่ตกลงกับเจ้าของลิขสิทธิ์ซอฟต์แวร์ไว้ล่วงหน้า การโอนเงินจ่ายค่าโฆษณาบนเว็บไซต์ โดยอัตโนมัติ ทันทีที่จำนวนคนดูถึงระดับที่ตกลงกับเจ้าของเว็บไซต์ไว้ล่วงหน้า การโอนคูปองส่วนลดราคาสินค้ามาให้ลูกค้าอัตโนมัติ ทันทีที่ถึงวันที่ใช้คูปอง นั้นได้ หรือ แม้แต่การโอนเงินจ่ายค่าบทความ ทันทีและทุกครั้งที่มีจำนวนผู้อ่าน บทความถึงระดับที่ตกลงกับนักเขียนไว้ล่วงหน้า トラバ ใดที่คู่สัญญาทุกฝ่าย ตกลงกันได้ เมื่อนั้นสัญญาอัจฉริยะ หรือ Smart Contract ก็จะถูกโปรแกรมและ บริหารจัดการอัตโนมัติด้วยโปรแกรมคอมพิวเตอร์บนเทคโนโลยี บล็อกเชน

ซึ่งในปัจจุบันบริษัท Ethereum และ Codius ได้เปิดใช้งาน สัญญาอัจฉริยะ บนพื้นฐานของเทคโนโลยี บล็อกเชน โดย The Ethereum Project เป็นหนึ่งตัวอย่างของการทำ สัญญาอัจฉริยะ เต็มรูปแบบซึ่งอยู่ในรูปแบบ ของ Public บล็อกเชนส่วนตัวอย่างอื่น ๆ นั้นเป็นการทำ สัญญาอัจฉริยะ ในรูปแบบของ บล็อกเชนส่วนตัว (Private Blockchain) หรือ บล็อกเชนแบบขออนุญาต (Permissioned Blockchain) ซึ่งจะทำการติดต่อ เฉพาะ โหนด ที่รู้จักและเชื่อถือได้เท่านั้น เพื่อเพิ่มความปลอดภัย การนำสัญญาอัจฉริยะ มาใช้งานนั้นสามารถช่วยแก้ปัญหาความไม่ไว้วางใจกันระหว่างคู่สัญญา การฉ้อโกง และการบิดเบือนสัญญา อีกทั้งยังสามารถ ช่วยแก้ปัญหาค่าความเสียหายในสัญญา ซึ่งมักจะเป็นข้อพิพาทระหว่างคู่สัญญาเสมอ ๆ เนื่องจากคู่สัญญาทั้งสองฝ่ายต่างตีความสัญญาคนละแบบ

ทั้งนี้ในการประยุกต์ใช้งาน สัญญาอัจฉริยะ ร่วมกับกระบวนการต่าง ๆ ที่เกี่ยวข้อง จำเป็นต้องทราบจุดเด่น และ ข้อจำกัดของ สัญญาอัจฉริยะ ที่เกี่ยวข้อง เพื่อให้สามารถนำ สัญญาอัจฉริยะ ไปใช้งานได้เหมาะสม โดยจุดเด่น ของ สัญญาอัจฉริยะ ประกอบไปด้วย

ความปลอดภัย (Security) เนื่องจาก สัญญาอัจฉริยะ ที่ถูกพัฒนา โดยใช้เทคโนโลยี บล็อกเชน นั้นจะถูกกระจายไป ยังสมาชิกอื่น ๆ ที่อยู่ในเครือข่าย จึงมั่นใจได้ว่า สัญญาอัจฉริยะ ดังกล่าวจะไม่สูญหาย หรือถูกเปลี่ยนแปลงเงื่อนไขการทำงานโดยไม่ได้รับอนุญาต

ความเป็นอัตโนมัติ (Automation) เนื่องจาก สัญญาอัจฉริยะ จะดำเนินการตามข้อตกลงโดยอัตโนมัติทันทีเมื่อเกิดเหตุการณ์ ตามเงื่อนไขในสัญญา ซึ่งได้มีการระบุไว้ล่วงหน้าแล้ว โดยไม่ต้อง มีคนกลางมาเกี่ยวข้อง

ความเป็นมาตรฐาน (Standardization) เนื่องจาก การนำ สัญญาอัจฉริยะ มาใช้งานในระบบใด ๆ นั้น หมายความว่าระบบนั้นจะต้อง ทำงานภายใต้เงื่อนไข หรือข้อตกลงต่างที่เป็นมาตรฐานเดียวกันทั้งระบบตามที่ได้กำหนดไว้ใน Smart Contract

ดังนั้นจากจุดเด่นของ สัญญาอัจฉริยะ ดังได้กล่าวมาแล้วข้างต้นลักษณะงาน ที่เหมาะสมสำหรับการนำ สัญญาอัจฉริยะ ไปประยุกต์ใช้ ประกอบไปด้วย

งานที่เกี่ยวข้องกับข้อมูลที่ไม่ต้องการให้แก้ไขได้ หรือสามารถเปลี่ยนแปลง เพิ่มเติมได้จากผู้ที่ได้รับอนุญาตเท่านั้น ยกตัวอย่างเช่น การเก็บข้อมูล สำหรับใช้ยืนยันบุคคล การเก็บข้อมูลสินทรัพย์ที่มีมูลค่าต่าง ๆ

งานที่ต้องการให้ธุรกรรมสามารถดำเนินการได้อย่างอัตโนมัติตาม เงื่อนไขที่กำหนด โดยปราศจากตัวกลางในการควบคุม หรือกำหนด การตัดสินใจ ยกตัวอย่างเช่น งานเกี่ยวกับการแลกเปลี่ยนสินทรัพย์

งานที่จำเป็นต้องเก็บประวัติการทำธุรกรรมที่เกี่ยวข้อง เพื่อใช้ในการสืบข้อมูลย้อนกลับ หรือตรวจสอบความถูกต้อง ยกตัวอย่างเช่น งานเก็บประวัติการรักษาทางการแพทย์ งานเก็บประวัติข้อมูล การถ่ายโอนสินทรัพย์ที่มีมูลค่า

งานที่ต้องการลดค่าใช้จ่ายกรณีมีตัวกลางร่วมในการบริหารจัดการระบบ ซึ่งสามารถประยุกต์ใช้ได้กับหลายหน่วยงานที่มีการใช้บุคลากร หรือสาขา ของสำนักงานในการดำเนินงานเป็นจำนวนมาก

2.3 อีเธอเรียม(Ethereum)

Ethereum เป็นบล็อกเชนแบบโอเพนซอร์สแบบกระจายศูนย์ที่มีฟังก์ชันสัญญาอัจฉริยะ Ether (ETH) เป็นโทเคนสกุลเงินดิจิทัลดั้งเดิมของแพลตฟอร์ม Ethereum เป็นสกุลเงินดิจิทัลที่ใหญ่เป็นอันดับสองตามมูลค่าตลาดรองจาก Bitcoin

Ethereum ได้รับการเสนอในปลายปี 2013 โดย Vitalik Buterin นักวิจัยและโปรแกรมเมอร์สกุลเงินดิจิทัล การพัฒนาได้รับทุนจากการขายออนไลน์ที่เกิดขึ้นระหว่างเดือนกรกฎาคมถึงสิงหาคม 2014 จากนั้นระบบจะเริ่มใช้งานจริงในวันที่ 30 กรกฎาคม 2015 โดยมีการสร้าง 72 ล้านเหรียญ Ethereum มีเครื่องเสมือนจำลองแบบกระจายอำนาจที่เรียกว่า Ethereum Virtual Machine (EVM) ซึ่งสามารถเรียกใช้สคริปต์โดยใช้เครือข่ายระหว่างประเทศของโหนดสาธารณะ ชุดคำสั่งของเครื่องเสมือนคือ Turing-complete ซึ่งตรงกันข้ามกับ Bitcoin

ในปี 2559 อันเป็นผลมาจากการใช้ประโยชน์จากข้อบกพร่องในซอฟต์แวร์สัญญาอัจฉริยะของโครงการ DAO และการขโมย Ether มูลค่า 50 ล้านดอลลาร์ในเวลาต่อมา Ethereum ได้ทำการ Hard Fork แบ่งออกเป็นสองบล็อกเชนแยกกัน โดยระบบแรกกลายเป็น Ethereum (ETH) ที่แก้ไขปัญหาช่องโหว่ในการโจรกรรมแล้ว และอีกระบบก็คงข้อมูลเดิมไว้กลายเป็น Ethereum Classic (ETC)

ขณะนี้ Ethereum กำลังพัฒนาและวางแผนที่จะใช้การอัปเดตชุดที่เรียกว่า Ethereum 2.0 ข้อกำหนดปัจจุบันสำหรับ Ethereum 2.0 รวมถึงการเปลี่ยนแปลงไปสู่การพิสูจน์การเดิมพันและการเพิ่มปริมาณธุรกรรมโดยใช้เทคโนโลยี Shard ซึ่งเป็นโครงสร้างฐานข้อมูลแบบหนึ่ง



รูปที่4 สัญลักษณ์ Ethereum

2.4 ระบบอินเทอร์เน็ตในทุกสิ่ง

ระบบอินเทอร์เน็ตในทุกสิ่ง หรือตัวย่อ IoT เป็นกรอบแนวคิดของระบบโครงข่ายที่รองรับการเชื่อมต่อกับอุปกรณ์หลากหลายชนิด ตั้งแต่ คอมพิวเตอร์ โทรศัพท์เคลื่อนที่ อุปกรณ์โครงข่าย อุปกรณ์อิเล็กทรอนิกส์ เซนเซอร์ และ วัตถุต่าง ๆ เข้าด้วยกัน อันเป็นผลให้ระบบต่าง ๆ สามารถ ติดต่อสื่อสารและทำงานร่วมกันได้อย่างเป็นอัตโนมัติทั้ง ยังเป็นผลให้มนุษย์สามารถเข้าถึงข้อมูลได้หลากหลายยิ่งขึ้น ควบคุมอุปกรณ์และระบบต่าง ๆ ได้อย่างมีประสิทธิภาพมากขึ้น

IoT อาจถือเป็นแนวคิดใหม่ที่มีการกล่าวถึงไม่นานมานี้ แต่ IoT เป็นผลสืบเนื่องของการพัฒนาระบบ อินเทอร์เน็ต ซึ่งมีวัตถุประสงค์เพื่อการสร้างโครงข่ายเพื่อเชื่อมโยงอุปกรณ์ที่มีมาตรฐานแตกต่างกันให้สามารถ สื่อสารกันได้ โดย IoT จะเปิดโอกาสให้มีการเชื่อมต่อในรูปแบบที่หลากหลายมากยิ่งขึ้น และรองรับอุปกรณ์ที่ พัฒนาโดยผู้ผลิตที่มีเทคโนโลยีแตกต่างกันมากกว่าเดิม ในปัจจุบันสามารถจัดกลุ่มการเชื่อมต่ออุปกรณ์ต่าง ๆ เข้า กับโครงข่ายอินเทอร์เน็ต ได้ตามรูปแบบดังต่อไปนี้

- การเชื่อมต่อผ่านอุปกรณ์สื่อสารระยะสั้น (Short-Range Devices) เป็นรูปแบบการเชื่อมต่ออุปกรณ์ในระยะสั้นมากโดยใช้กำลังส่งต่ำมาก เหมาะสำหรับสื่อสารในพื้นที่ครอบคลุมขนาดเล็ก ซึ่งอยู่ในลักษณะ การเชื่อมต่อระหว่างอุปกรณ์ (peer-to-peer) หรือ การเชื่อมต่อแบบโครงข่ายก็ได้ ตัวอย่างของการ เชื่อมต่อในลักษณะดังกล่าวได้แก่ WiFi, Bluetooth, Z-Wave, ZigBee ฯลฯ
- การเชื่อมต่อผ่านโครงข่ายโทรศัพท์เคลื่อนที่ เป็นรูปแบบการให้บริการที่มีพื้นที่ครอบคลุมกว้าง โดยอาศัย การเชื่อมต่ออุปกรณ์เครื่องลูกข่าย IoT เข้ากับโครงสร้างพื้นฐานของระบบโทรศัพท์เคลื่อนที่ที่มีอยู่แล้ว ตัวอย่างของการ เชื่อมต่อในลักษณะดังกล่าวได้แก่ เทคโนโลยี NB-IoT และ LTE-M
- การเชื่อมต่อผ่านโครงข่าย LPWAN เป็นรูปแบบการเชื่อมต่อผ่านโครงข่ายกำลังส่งต่ำบริเวณกว้าง Low Power Wide Area Network (LPWAN) โดยเน้นใช้งานในลักษณะการสื่อสารแบบ Narrow Band หรือ Ultra Narrow Band ที่มีอัตราการส่งข้อมูลต่ำมาก ประหยัดพลังงานมาก และมีราคาอุปกรณ์ต่อหน่วยที่ต่ำ ตัวอย่างของการ เชื่อมต่อในลักษณะดังกล่าวได้แก่ LoRaWAN, SigFox, และ Ingenu ฯลฯ
- การเชื่อมต่อผ่านข่ายสื่อสารดาวเทียม ซึ่งมีเหมาะสมกับการใช้งานที่มีพื้นที่ครอบคลุมการให้บริการที่กว้าง มาก แต่การเชื่อมต่องานดังกล่าวจะมีระยะเวลาการตอบสนอง (latency) ที่ช้ากว่าการเชื่อมต่อรูปแบบอื่น ๆ เนื่องจากระยะเวลาที่สัญญาณเดินทาง ไป-กลับ ระหว่างอุปกรณ์สื่อสารภาคพื้นโลกและดาวเทียม

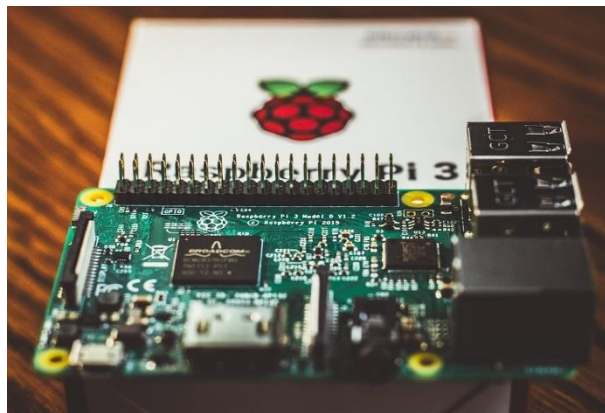
3 เครื่องมือที่ใช้ในการทำโครงการ

3.1 ฮาร์ดแวร์

3.1.1 คอมพิวเตอร์ (Computer)

3.1.2 ราสเบอร์รี่พาย (Raspberry Pi)

เป็นบอร์ดคอมพิวเตอร์ขนาดเล็ก มีขนาดใกล้เคียงกับบัตรเครดิต มีระบบปฏิบัติการเฉพาะของตัวเอง มีขา GPIO (General Purpose Input/Output) สำหรับติดต่อสื่อสารกับวงจรอิเล็กทรอนิกส์ภายนอกได้ และยังสามารถต่อชุดหน่วยความจำ ชุดอินพุต เอาต์พุต อาทิ เช่น แม้าส์ คีย์บอร์ด และ จอแสดงผลเพื่อใช้งานลักษณะเดียวกับคอมพิวเตอร์ได้



รูปที่5 ราสเบอร์รี่พาย

ที่มา: <https://www.scimath.org/article-technology/item/9104-raspberry-pi>

3.1.3 มิเตอร์ไฟฟ้าอัจฉริยะ (Smart meter)

Smart Meter มาเชื่อมกับสัญญาณอัจฉริยะด้วยเหตุผลที่ว่า ในปัจจุบันมิเตอร์ในการเก็บค่าไฟนั้นอยู่ในรูปของจานหมุนและให้เจ้าหน้าที่ทำการอ่านค่าด้วยสายตาและนำไปกรอกใส่ในระบบ ซึ่งการอ่านด้วยตาจะทำให้เกิดความคลาดเคลื่อนได้ง่าย จึงเป็นที่มาของ มิเตอร์ไฟฟ้าอัจฉริยะ ที่จะเก็บข้อมูลแล้วแสดงออกมาเป็นตัวเลขให้เห็นได้เลยทำให้การอ่านที่คลาดเคลื่อนนั้นไม่เกิดขึ้น



รูปที่6 มิเตอร์ไฟฟ้าอัจฉริยะ

ที่มา: <https://brandinside.asia/smart-meter-smart-grid-iot-technology/>

3.1.4 รีเลย์ (Relay)

เป็นอุปกรณ์ที่เปลี่ยนพลังงานไฟฟ้าให้เป็นพลังงานแม่เหล็กเพื่อใช้ในการดึงดูดหน้าสัมผัสของคอนแทคให้เปลี่ยนสถานะโดยการป้อนกระแสไฟฟ้าให้กับขดลวดเพื่อทำการปิดหรือเปิดหน้าสัมผัสคล้ายกับสวิตช์อิเล็กทรอนิกส์ซึ่งเราสามารถนำรีเลย์ไปประยุกต์ใช้ในการควบคุมวงจรต่างๆในงานช่างอิเล็กทรอนิกส์มากมาย

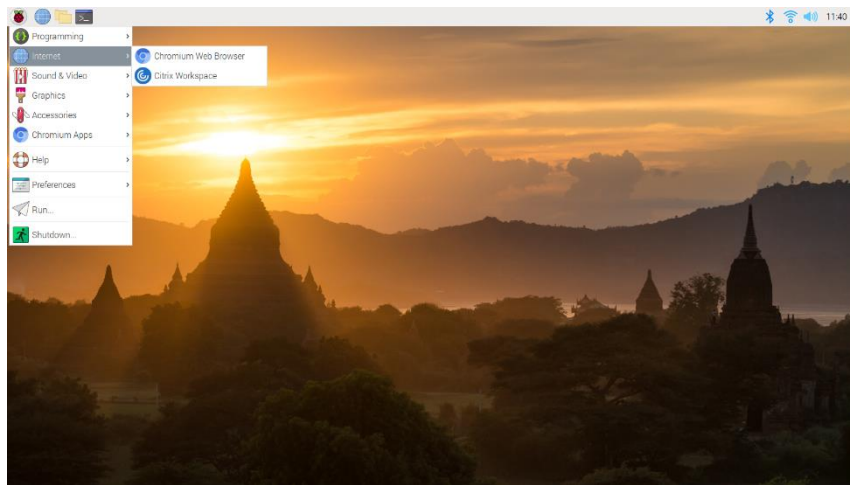
3.2 ซอฟต์แวร์

3.2.1 ภาษา Python

เป็นภาษาสำหรับเขียนคำสั่งเพื่อดึงข้อมูลจาก สัญญาอัจฉริยะ ซึ่งจะเขียนบน ราสเบอร์รี่พาย

3.2.2 Raspbian

เป็นระบบปฏิบัติการสำหรับติดตั้งใช้งานบนบอร์ด ราสเบอร์รี่พาย



รูปที่7 ระบบปฏิบัติการ Raspbian

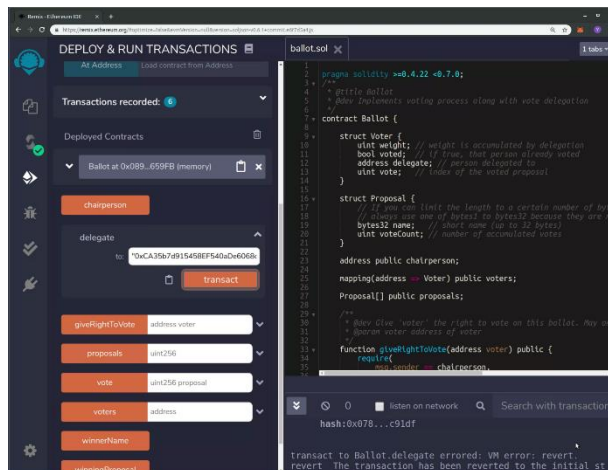
ที่มา: https://en.wikipedia.org/wiki/Raspberry_Pi_OS

3.2.3 ภาษา Solidity

เป็นภาษาสำหรับการเขียนสัญญาอัจฉริยะหรือ Smart Contract

3.2.4 Remix-ide

เป็น เว็บไซต์สำหรับการพัฒนาและทดสอบ สัญญาอัจฉริยะหรือ Smart Contract โดยรองรับการเขียน ภาษา Solidity



รูปที่8 หน้าเว็บไซต์ remix-ide

ที่มา: <https://remix-project.org/>

3.2.5 Metamask

เป็นกระเป๋าเงิน Ethereum แบบโอเพนซอร์ส ที่รองรับโทเคน (Token) ที่อยู่บน Ethereum



รูปที่9 logo Metamask

ที่มา: <https://bitcoinaddict.org/2020/09/14/how-to-use-metamask/>

3.2.6 MyEtherWallet

MEW คือโปรแกรมอินเทอร์เน็ตแบบ Open-source เพื่อสร้างกระเป๋าอีเธอร์เรียม (ETH) โดยทำงานร่วมกับอีเธอร์เรียม บล็อกเชน (Ethereum blockchain) ซึ่งใช้ระบบตรวจสอบตัวตนแบบง่ายๆ เพื่อล็อกอินเข้าสู่กระเป๋า



รูปที่ 10 logo MyEtherWallet

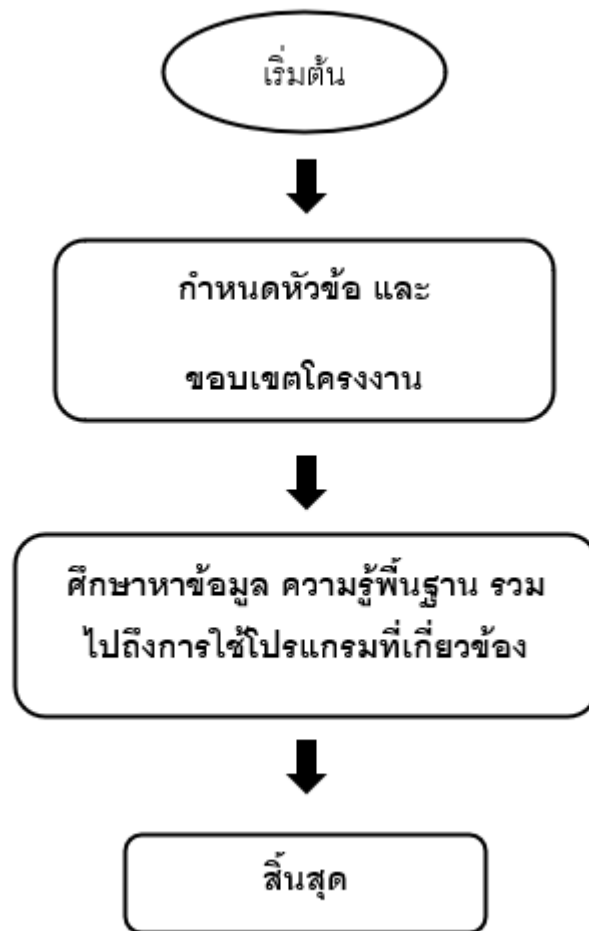
ที่มา: <https://ethereumworldnews.com/ethereum-eth-mewconnect-digital-wallet-application-launched-by-myetherwallet-on-ios/>

4 วิธีการดำเนินโครงการ

4.1 กระบวนการรวบรวมข้อมูล

4.1.1 กำหนดหัวข้อและขอบเขตในการจัดทำโครงการ

4.1.2 ศึกษาหาข้อมูล ความรู้พื้นฐาน รวมไปถึงการใช้โปรแกรมที่เกี่ยวข้อง



รูปที่ 11 แผนภาพขั้นตอนกระบวนการรวบรวมข้อมูล

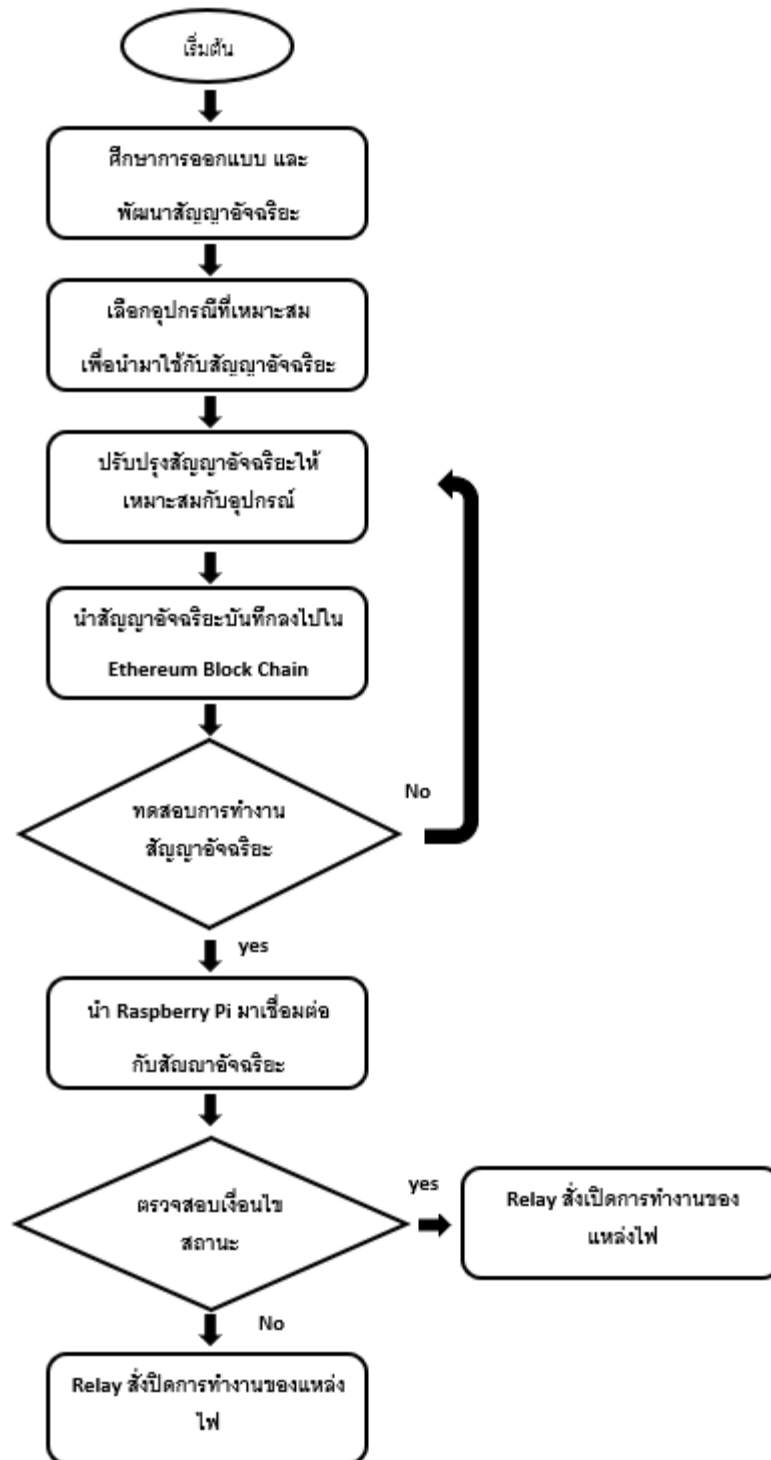
4.2 กระบวนการศึกษาข้อมูล

4.2.1 ทำการศึกษาออกแบบ และพัฒนาสัญญาอัจฉริยะ รวมถึงกระบวนการเชื่อมต่อข้อมูลเพื่อดึงค่ามาจากสัญญาอัจฉริยะ เพื่อนำไปออกแบบเงื่อนไขในอุปกรณ์ IoT

4.2.2 ทดลองใช้สัญญาอัจฉริยะในระบบ test net เพื่อดูความสามารถ และความถูกต้องของการทำงานของสัญญาอัจฉริยะ

4.2.3 ทดลองการเชื่อมต่อระบบ IoT กับสัญญาอัจฉริยะ โดยมี micro controller (Raspberry pi 4) เป็นตัวกลางการเชื่อมต่อ

4.2.4 วิเคราะห์ และสรุปผลจากการทดลองและออกแบบ



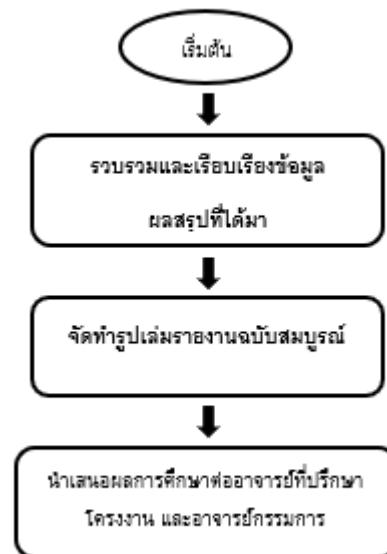
รูปที่ 12 แผนภาพขั้นตอนกระบวนการศึกษาข้อมูล

4.3 กระบวนการนำเสนอและจัดทำรูปเล่มรายงาน

4.3.1 รวบรวมและเรียบเรียงข้อมูลผลสรุปการศึกษาที่ได้มา

4.3.2 จัดทำรูปเล่มรายงานฉบับสมบูรณ์

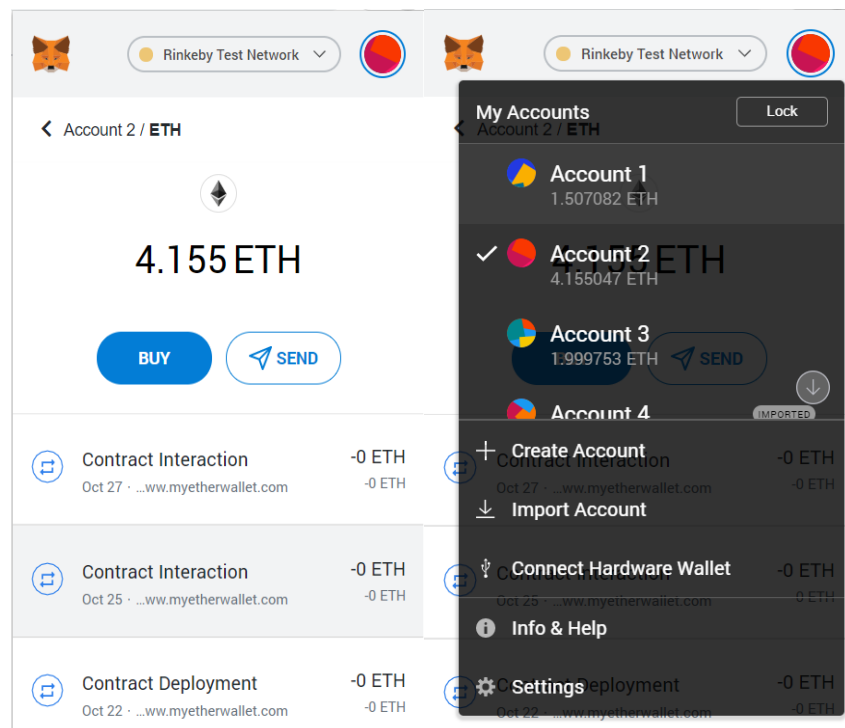
4.3.3 นำเสนอผลการศึกษาต่ออาจารย์ที่ปรึกษาโครงงาน และอาจารย์กรรมการ



รูปที่ 13 แผนภาพขั้นตอนกระบวนการนำเสนอ และจัดทำรูปเล่มรายงาน

5 ผลการดำเนินโครงการและวิจารณ์

ในส่วนของการดำเนินงานทางผู้จัดทำได้พัฒนาระบบสัญญาอัจฉริยะที่จะต้องทำงานอยู่บน Ethereum โดย เครือข่ายบล็อกเชน(Blockchain Network) ที่เลือกใช้ จะเป็น เครือข่ายทดสอบ (Test Network) ชื่อว่า Rinkeby Test Network โดยจะทำการใช้ Metamask เป็นกระเป๋าที่จะทำการเก็บ Ether ซึ่งเป็นหน่วยเงินดิจิทัลของ Ethereum ซึ่ง Metamask จะทำหน้าที่นอกจากเป็นกระเป๋าเงินดิจิทัลแล้ว ยังสามารถจัดการบัญชีของผู้ใช้งานที่จะต้องทำการติดต่อ และเรียกใช้กับ สัญญาอัจฉริยะ ซึ่งสามารถตรวจสอบรายละเอียดใช้งานได้



รูปที่ 14 บัญชี Metamask เลือกใช้ Rinkeby Test Network

5.1 ผลการออกแบบพัฒนาสัญญาอัจฉริยะ

การพัฒนาอัลกอริทึมการทำงานของ สัญญาอัจฉริยะ ได้ใช้ Remix-ide ที่เป็น browser-based IDE ช่วยในการพัฒนาและทดสอบ โดยภาษาที่ใช้ในการเขียนอัจฉริยะ คือ Solidity โดย

5.1.1 องค์ประกอบของโค้ดสัญญาอัจฉริยะ

โดยในองค์ประกอบของสัญญาอัจฉริยะจะมีส่วนประกอบด้วยกัน 2 ส่วนหลัก ๆ คือ ส่วนของการประกาศ สัญญา และ ค่า ตัวแปรต่าง ๆ และส่วนของการประกาศฟังก์ชัน ในส่วนของการประกาศค่าตัวแปรนั้นจะประกาศค่าที่เป็นตัวอย่างเช่น

- TokenElec เป็นชื่อของ สัญญา
- balanceOf ตัวแปรที่จะทำการรับค่า address ของบัญชีผู้ใช้และคืนค่าออกมาเป็น uint หรือค่า จำนวน โทเคนในกระเป๋าตัวเอง
- PaymentDetail เป็นตัวแปรแบบ Struct จะทำการเก็บตัวแปรย่อย ได้แก่ address ของ ผู้ใช้ address ของผู้ทำการ deployed สัญญาอัจฉริยะ และค่า value จำนวน โทเคน และ สถานการณ์จ่ายธุรกรรม
- Constructor เป็นตัวแปรที่จะรับค่าและกำหนดค่าที่รับเป็นจำนวนโทเคน ให้กับผู้ที่ทำการ deploy สัญญา

```
pragma solidity ^0.5.2;

contract TokenElec {
    mapping (address => uint256) public balanceOf;
    mapping (address => uint256) public yourcost;
    mapping (address => string) public status;
    mapping (address => PaymentDetail) public transaction;
    struct PaymentDetail {
        address customer;
        address ownerE;
        uint value;
        bool status_payment;
    }
    constructor(uint256 initialSupply) public {
        balanceOf[msg.sender] = initialSupply;
    }
}
```

รูปที่ 15 โค้ดของสัญญาอัจฉริยะส่วนของการประกาศตัวแปร

ต่อมาใน ส่วนของการประกาศฟังก์ชัน จะประกอบด้วย ฟังก์ชัน การโอน การตั้งค่าการใช้บริการแก่แต่ละบัญชี และ ฟังก์ชันการ ซื้อโทเคนเพื่อจะนำมาชำระการใช้จ่ายธุรกรรม โดยจะมีแค่ฟังก์ชันการตั้งค่าการใช้บริการเท่านั้นที่จะใช้ได้แค่ ผู้ที่ทำการ deploy สัญญาลงไป

```
function setprice(address _customer,uint _cost ) public {
    require(msg.sender == 0x5408142593bA953843811B245703977085995558C);
    yourcost[_customer] = _cost;
    status[_customer] = "You have to pay :(";
}

function BuyToken(address _to, uint256 _value) public returns (bool success){
    balanceOf[_to] += _value;
    return true;
}

function transfer(address _from, address _to, uint256 _value) public returns (bool success) {
    require ( _value == yourcost[_from]);
    require(balanceOf[_from] >= _value);          // Check if the sender has enough
    require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows

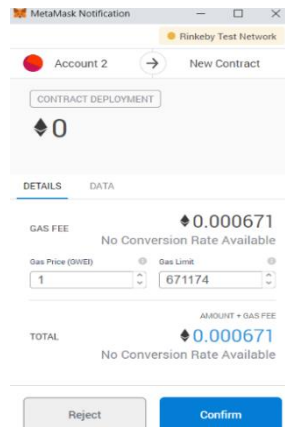
    balanceOf[_from] -= _value;
    balanceOf[_to] += _value;
    status[_from] = "You already paid :)";
    yourcost[_from] = 0;

    PaymentDetail storage point = transaction[_from];
    point.customer = _from;
    point.ownerE = _to;
    point.value = _value;
    point.status_payment = true;
    return true;
}
```

รูปที่ 16 โค้ดของสัญญาอัจฉริยะส่วนของการประกาศฟังก์ชัน

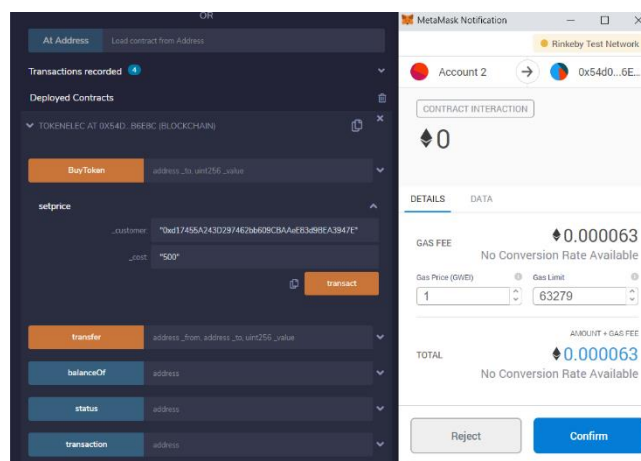
5.2 ผลการทดสอบการทำงานสัญญาอัจฉริยะ

หลังจากทำการออกแบบ สัญญาเสร็จแล้วจะทำการ Deploy เพื่อทดสอบการทำงานของฟังก์ชันและการเชื่อมต่อของสัญญาอัจฉริยะกับ Rinkeby Test Network โดยในการ Deploy สัญญาลงเครือข่ายและการทำรายการธุรกรรมเรียกใช้ฟังก์ชันบางฟังก์ชัน จะต้องเสียค่าธรรมเนียม เรียกว่าค่า Gas ซึ่งค่าจะมีปริมาณแปรผันตามการเรียกใช้และเข้าถึงข้อมูลในบล็อกเชน ซึ่ง Gas จะจ่ายเป็น Ether หรือคือเงิน ETH นั้นเอง

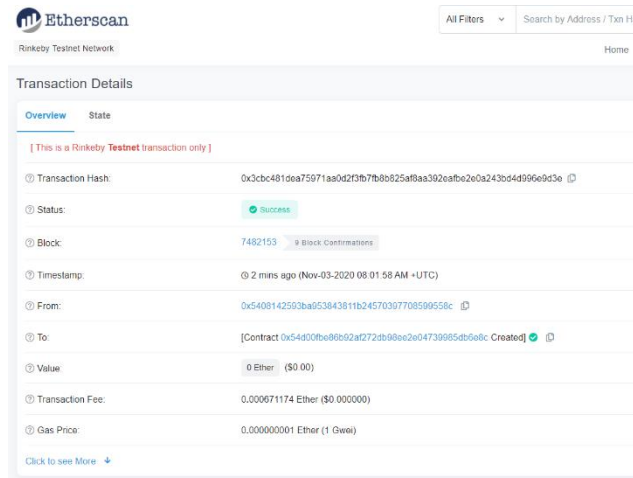


รูปที่ 17 ค่า Gas ในการ Deploy สัญญาอัจฉริยะ

ซึ่ง Remix-ide จะทำการแสดง สัญญาอัจฉริยะที่ Deploy ลงไปแล้วซึ่งจะ มีการแสดง รหัสที่อยู่ของสัญญานั้นเพื่อจะสามารถตรวจสอบรายละเอียดการทำงานและธุรกรรมได้ในเว็บไซต์ Etherscan.io ได้



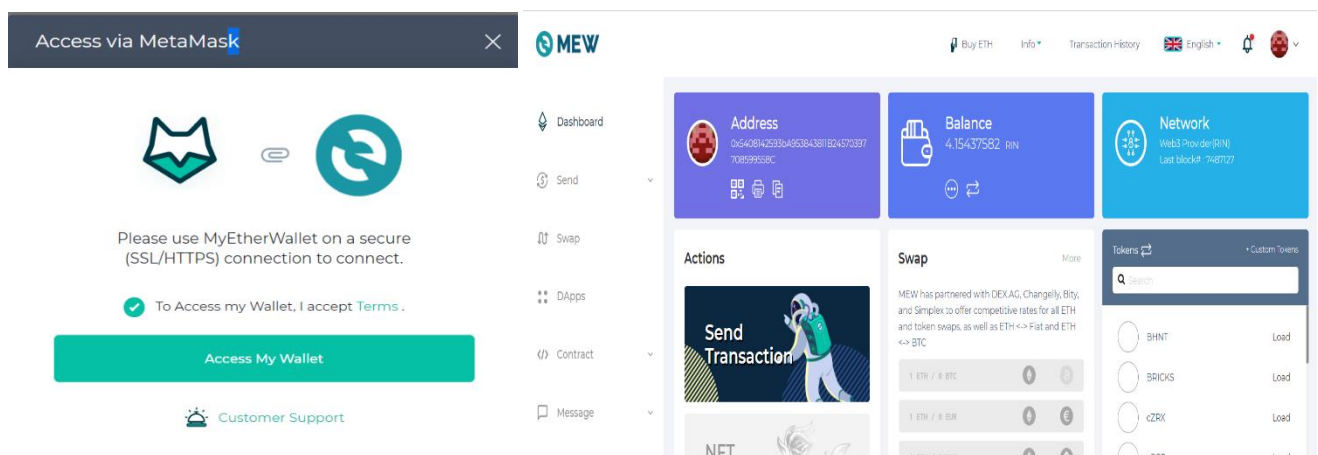
รูปที่ 18 การทดสอบ สัญญาอัจฉริยะใน Remix-ide



รูปที่ 19 รายละเอียดธุรกรรม ของการ Deploy สัญญาอัจฉริยะที่ตรวจสอบโดย
ใช้รหัสที่อยู่ของสัญญาในเว็บไซต์ Etherscan.io

5.3 ผลการนำสัญญาอัจฉริยะมาลงเว็บไซต์ที่สามารถเรียกใช้งานฟังก์ชันการทำงาน

ในการนำสัญญาอัจฉริยะมาเชื่อมเข้าสู่เว็บไซต์ที่มีหน้า interface การใช้งาน ทางผู้จัดทำได้ MyEtherWallet ซึ่งเป็นโปรแกรมอินเทอร์เฟซแบบ Open-source มาใช้งาน ซึ่ง MyEtherWallet สามารถเชื่อมต่อบัญชีผู้ใช้มาจาก Metamask ได้โดยจะสามารถแสดงข้อมูลบัญชี และ จำนวนเงิน Ether ได้



รูปที่ 20 การเชื่อมต่อ MyEtherWallet กับ Metamask และข้อมูลบัญชี

5.3.1 ผลการนำสัญญาอัจฉริยะมา Deploy ลงใน MyEtherWallet

ในการที่จะ Deploy สัญญาอัจฉริยะ ลง MyEtherWallet จะต้องใช้องค์ประกอบ 3 อย่างคือ

- ByteCode คือ การแปลงซอร์สโค้ดในภาษา solidity ให้กลายเป็นรหัสภาษากลาง โดยใน remix-ide จะทำการสร้างมาให้หลังที่โค้ดถูก Compile
- ABI/JSON Interface ย่อมาจาก Application Binary Interface โดยผู้พัฒนา Smart Contract จะได้รับ ABI จากการ Compile แล้วนำไปแจกจ่ายให้ ผู้ใช้งาน โดย ผู้ใช้งาน จะเอา ABI ไปใช้กับ MyEtherWallet เพื่อส่งคำสั่งหา Smart Contract
- Contract Name เป็นชื่อของสัญญาอัจฉริยะ

Deploy Contract

Byte Code Clear Copy

090565b9056fea265627a7a7231582018be11683792b8a072ecd83a4144861e42ae1ad766aa0acda65a27d969cccb5564736f6c63430005110032",
"opcodes": "PUSH1 0x80 PUSH1 0x40 MSTORE CALLVALUE DUP1 ISZERO PUSH2 0x10 JUMPI PUSH1 0x0 DUP1 REVERT

ABI/JSON Interface Clear Copy

```
{  "payable": false,  "stateMutability": "nonpayable",  "type": "constructor",}, {  "constant": false,  "inputs": [    {      "internalType": "address",      "name": "to",      "type": "address"    }  ],  "outputs": [],  "payable": false,  "stateMutability": "nonpayable",  "type": "function"}
```

Constructor Inputs:

InitialSupply (uint256):

0

Contract Name

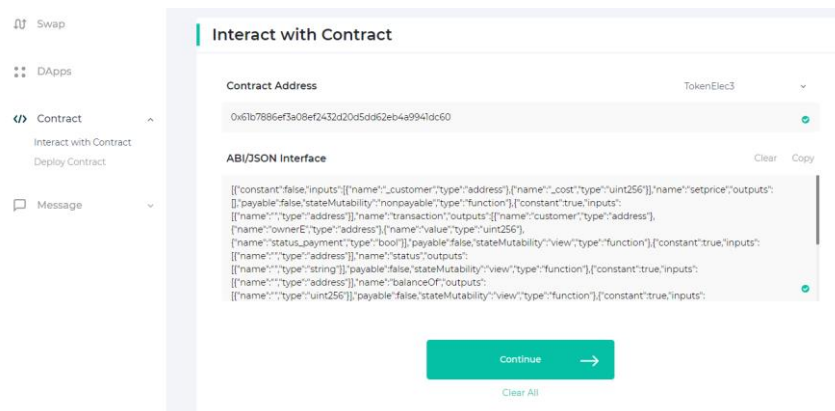
TokenEled

Sign Transaction

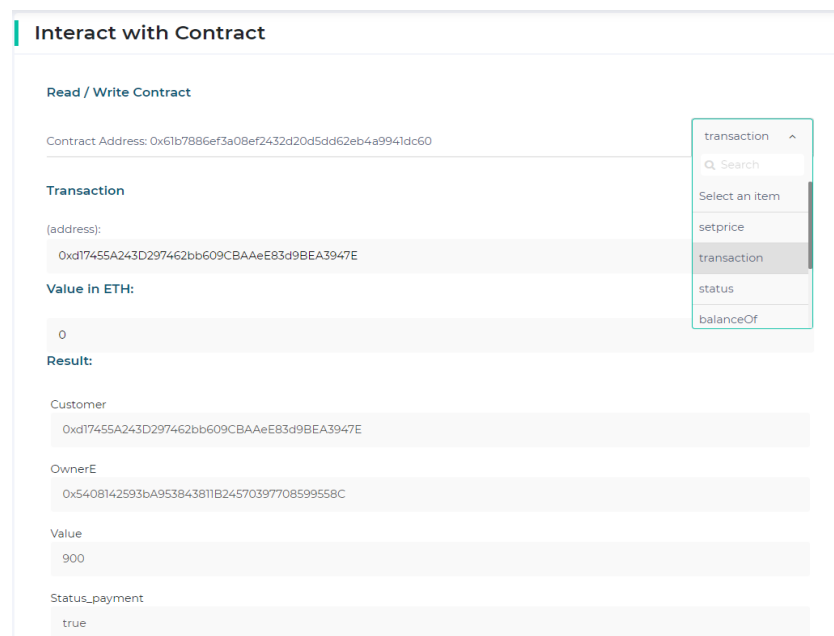
รูปที่ 21 การนำสัญญาอัจฉริยะมา Deploy ลงใน MyEtherWallet

5.3.2 ผลการติดต่อสัญญาอัจฉริยะมาใน MyEtherWallet

เมื่อสัญญาอัจฉริยะถูก Deploy แล้วเราก็จะได้ Contract Address มาซึ่งเป็นรหัสที่อยู่ของสัญญานั้นใน Ethereum Network โดยในการ ติดต่อนั้นเราจะต้องใช้ Contract Address และ ABI/JSON Interface จากนั้นเราก็จะสามารถเข้าถึงสัญญาอัจฉริยะได้และเรียกใช้ฟังก์ชันการทำงานรวมถึงอ่านค่าข้อมูลเพื่อตรวจเงื่อนไขในสัญญาอัจฉริยะนั้นได้



รูปที่ 22 การติดต่อสัญญาอัจฉริยะมาใน MyEtherWallet



รูปที่ 23 การเรียกฟังก์ชันและทดสอบการทำงาน สัญญาอัจฉริยะใน MyEtherWallet

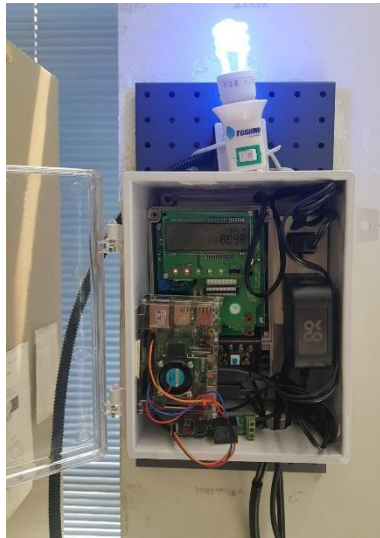
5.4 ผลการเชื่อมต่อ สัญญาณจลริยะเข้ากับระบบไอโอที

ในการดึงข้อมูลจากสัญญาณจลริยะ เพื่อควบคุมการทำงานของมิเตอร์จลริยะ เราได้เขียนโปรแกรมภาษา python ซึ่งจะทำงานอยู่บนรหัสเบอร์รี่พายโดยจะดึงข้อมูลในสัญญาณจลริยะเพื่อทำควบคุมการทำงานของ รีเลย์กับรหัสเบอร์รี่พาย ให้ควบคุมการจ่ายไฟฟ้าเข้า มิเตอร์จลริยะ ตามเงื่อนไขที่ได้กำหนดไว้ในสัญญาณจลริยะ



รูปที่ 24 รหัสเบอร์รี่พายที่ต่อกับรีเลย์เพื่อควบคุมมิเตอร์จลริยะ

- เมื่อข้อมูลที่อ่านได้จากสัญญาณจลริยะเป็นการกำหนดสั่งให้จ่ายไฟ รัสเบอรรี่พาย จะสั่งให้รีเลย์จ่ายไฟเข้ากับ มิเตอร์จลริยะเพื่อให้อุปกรณ์ไฟฟ้าทำงาน



รูปที่ 25 รัสเบอรรี่พายที่สั่งรีเลย์จ่ายไฟเข้ามิเตอร์จลริยะ

- เมื่อข้อมูลที่อ่านได้จากสัญญาณจลริยะเป็นการกำหนดสั่งให้ตัดไฟ รัสเบอรรี่พาย จะสั่งให้รีเลย์ตัดไฟมิเตอร์จลริยะ



รูปที่ 26 รัสเบอรรี่พายที่สั่งรีเลย์ตัดไฟมิเตอร์จลริยะ

6 สรุปผลการดำเนินงานและข้อเสนอแนะ

การประยุกต์ใช้สัญญาอัจฉริยะเพื่อควบคุมอุปกรณ์ไอโอทีบนเครือข่ายบล็อกเชน ที่ได้จัดทำขึ้นนั้น ได้มีการออกแบบให้เหมาะกับการใช้งานของอุปกรณ์ไอโอทีให้ปลอดภัยและยากต่อการบิดเบือนข้อมูลเนื่องจากการกำหนดเงื่อนไขผู้ที่ได้รับอนุญาตเท่านั้น (ผู้ให้บริการระบบ) ที่จะสามารถปรับเปลี่ยนเพื่อควบคุมสถานะของคนอื่นที่เป็นผู้ใช้บริการได้และเมื่อสถานะมีการเปลี่ยนแปลงจะมีสัญญาณเตือนเพื่อให้ผู้ใช้บริการทราบถึงการตรวจสอบสถานะโดยสรุปองค์ประกอบการทำงานในระบบได้ 3 อย่างคือ

1. การทำงานของฟังก์ชันในสัญญาอัจฉริยะ

- BuyToken :** เป็นคำสั่งที่ใช้ในการสั่งซื้อเหรียญที่เป็นหน่วยในการคิดราคาค่าไฟฟ้าจากหน่วยงาน
- BalanceOf :** เป็นคำสั่งที่ใช้ในการตรวจสอบยอดคงเหลือของ Token ของเรา
- Yourcost :** เป็นคำสั่งที่ใช้ในการตรวจสอบยอดรายจ่ายค่าไฟฟ้าของเดือนนี้
- status :** เป็นคำสั่งที่ใช้ในการตรวจสอบสถานะการจ่ายค่าไฟฟ้าว่าจ่ายแล้วหรือยัง
- Setprice :** เป็นคำสั่งเฉพาะที่จะสามารถในการกำหนดราคาค่าไฟฟ้าหน่วยเป็น Token ให้กับผู้ใช้ซึ่งฟังก์ชันนี้มีเพียงผู้ให้บริการเท่านั้นที่สามารถเรียกใช้ฟังก์ชันนี้ได้
- Transfer :** เป็นคำสั่งในการโอน Token เพื่อชำระค่าไฟฟ้าไปยังผู้ให้บริการ

2. การเรียกใช้คำสั่งของสัญญาอัจฉริยะ

การเรียกใช้คำสั่งจะเรียกผ่านทางเว็บไซต์ **MyEtherWallet** ที่เชื่อมต่อกับ **MetaMask** ที่ทำหน้าที่เหมือนกระเป๋าสตางค์ในการเก็บเงินของเรา

3. การนำสัญญาอัจฉริยะที่อยู่บนบล็อกเชนมาเชื่อมกับระบบไอโอที

การดึงค่าคำสั่งที่อยู่ในสัญญาอัจฉริยะซึ่งมีการกำหนดเงื่อนไขไว้ ผ่านรหัสเบอริ์พายเพื่อควบคุมการทำงานของรีเลย์ที่จะทำการจ่ายและตัดไฟมิเตอร์อัจฉริยะ

ข้อเสนอแนะ

การเรียกใช้งานผ่านทางเว็บไซต์ **MyEtherWallet** สามารถเปลี่ยนไปใช้ เว็บไซต์หรือแอปพลิเคชันบน smart phone ที่เราสามารถเขียนขึ้นมาเองได้

7 บรรณานุกรม

- [1] K.Qiao, H.Tang, W.You, Y.Zhao.(2019, April 12).Blockchain Privacy Protection Scheme Based on AggregateSignature.(4th edition).[Online].4(5).Available:<https://ieeexplore.ieee.org/document/8725693>[july 14, 2020]
- [2] X.Li, Y.Mei, J.Gong, F.Xiang, Z.Sun.(2020, April 14).A Blockchain Privacy Protection Scheme Based onRingSignature.(1st edition).[On-line].10(5).Available :[https://ieeexplore.ieee.org /document/-9066964](https://ieeexplore.ieee.org/document/-9066964)[july 14, 2020]
- [3] W.Zheng,AZ.Zheng,AX.Chen,AK.Dai,AP.Li, R.Chen.(2019, August 11).A Blockchain-as-a-Service Platform.(5th edition).[On-line].7(5).vailable:<https://ieeexplore.ieee.org/document/-8840920/references#references>[july 12, 2020]
- [4] Digital Government Development Agency (Public Organization) (DGA).(2019,January 13). Blockchain ofgovernmentsservices.(1stedition).[On-line].1(3).vailable:
https://www.dga.or.th/upload/download/file_ff487bacfb3198a615ca75112b8d156c.pdf
- [5] Wikipedia(2015,July30).Ethereum.(1stedition).[On-line].7(3).vailable:
<https://en.wikipedia.org/wiki/Ethereum>

ประวัตินิติ

1. ชื่อ-นามสกุล นาย ปาพจน์ บุษราคัม เลขประจำตัวนิติ 6010501229

ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

ที่อยู่ปัจจุบัน 157/75 หมู่บ้านพูนสินธานี 1 เคหะร่มเกล้า 64 คลองสองต้นนุ่น ลาดกระบัง กรุงเทพมหานคร 10520

โทรศัพท์ที่บ้าน 02-918-3203 โทรศัพท์เคลื่อนที่ 089-219-9449

E-mail paphot.b@ku.th

ระดับการศึกษา:ปริญญาตรี

คุณวุฒิการศึกษา	จากโรงเรียน/สถาบัน	ปีการศึกษาที่จบ
มัธยมศึกษาตอนปลาย	เตรียมอุดมศึกษาพัฒนาการ	พ.ศ.2559
มัธยมศึกษาตอนต้น	จุฬารณราชวิทยาลัย ชลบุรี	พ.ศ.2556

2. ชื่อ-นามสกุล นาย วัชรพงษ์ จิตติประเสริฐ เลขประจำตัวนิติ 6010501342

ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

ที่อยู่ปัจจุบัน 41 นาคนิवास 37 แยก 1-4 ลาดพร้าว ลาดพร้าว กรุงเทพมหานคร 10230

โทรศัพท์ที่บ้าน 02-956-1634 โทรศัพท์เคลื่อนที่ 087-327-9950

Email Vatcharapong.j@ku.th

ระดับการศึกษา:ปริญญาตรี

คุณวุฒิการศึกษา	จากโรงเรียน/สถาบัน	ปีการศึกษาที่จบ
มัธยมศึกษาตอนปลาย	โรงเรียนกรุงเทพคริสเตียนวิทยาลัย	พ.ศ.2559
มัธยมศึกษาตอนต้น	โรงเรียนกรุงเทพคริสเตียนวิทยาลัย	พ.ศ.2556