**ระบบการลงคะแนนเสียงแบบอิเล็กทรอนิกส์**

**โดยใช้บล็อคเชนแบบส่วนตัว**

**(Electronic Vote By Private Blockchain)**

**โดย**

**กานต์ เนียมจันทร์**

**KARN NIAMCHAN**

**อภิชัย ตันตสิรินทร์**

**APICHAI TANTASIRIN**

**อาจารย์ที่ปรึกษา**

**ผศ.ดร.ปานวิทย์ ธุวะนุติ**

**ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตร์บัณฑิต**

**สาขาวิชาเทคโนโลยีสารสนเทศ**

**คณะเทคโนโลยีสารสนเทศ**

**สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง**

**ภาคเรียนที่ 1 ปีการศึกษา 2560**

**ระบบการลงคะแนนเสียงแบบอิเล็กทรอนิกส์**

**โดยใช้บล็อคเชนแบบส่วนตัว**

**(Electronic Vote By Private Blockchain)**

**โดย**

**กานต์ เนียมจันทร์**

**KARN NIAMCHAN**

**อภิชัย ตันตสิรินทร์**

**APICHAI TANTASIRIN**

**อาจารย์ที่ปรึกษา**

**ผศ.ดร.ปานวิทย์ ธุวะนุติ**

**ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตร์บัณฑิต**

**สาขาวิชาเทคโนโลยีสารสนเทศ**

**คณะเทคโนโลยีสารสนเทศ**

**สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง**

**ภาคเรียนที่ 1 ปีการศึกษา 2560**

**Electronic Vote By Private Blockchain**

**KARN NIAMCHAN**

**APICHAI TANTASIRIN**

**A PROJECT SUBMITTED IN PARTIAL FULFILLMENT**

**OF THE REQUIREMENT FOR THE DEGREE OF**

**BACHELOR OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY FACULTY OF INFORMATION TECHNOLOGY**

**KING MONGKUT’S INSTITUTE OF TECHNOLOGY LADKRABANG**

**1/2017**

**COPYRIGHT 2017**

**FACULTY OF INFORMATION TECHNOLOGY**

**KING MONGKUT’S INSTITUTE OF TECHNOLOGY LADKRABANG**

**ใบรับรองปริญญานิพนธ์ ประจำปีการศึกษา 2560**

**คณะเทคโนโลยีสารสนเทศ**

**สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง**

**เรื่อง ระบบการลงคะแนนเสียงแบบอิเล็กทรอนิกส์โดยใช้บล็อกเชนแบบส่วนตัว**

**ELECTRONIC VOTE BY PRIVATE BLOCKCHAIN**

**ผู้จัดทำ**

1. **นายกานต์ เนียมจันทร์ รหัสนักศึกษา 57070004**
2. **นายอภิชัย ตันตสิรินทร์ รหัสนักศึกษา 57070142**

**…………………………………… อาจารย์ที่ปรึกษา**

**(ผศ.ดร.ปานวิทย์ ธุวะนุติ)**

**ใบรับรองโครงงาน (Project)**

**เรื่อง**

**ระบบการลงคะแนนเสียงแบบอิเล็กทรอนิกส์โดยใช้บล็อคเชนแบบส่วนตัว**

**Electronic Vote By Private Blockchain**

**นายกานต์ เนียมจันทร์ รหัสนักศึกษา 57070004**

**นายอภิชัย ตันตสิรินทร์ รหัสนักศึกษา 57070142**

ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ

การศึกษาวิชาโครงงาน หลักสูตรวิทยาศาสตร์บัณฑิต (เทคโนโลยีสารสนเทศ)

ภาคเรียนที่ 1 ปีการศึกษา 2560

……………………………………

(นายกานต์ เนียมจันทร์)

……………………………………

(นายอภิชัย ตันตสิรินทร์)

**หัวข้อโครงงาน** ระบบการลงคะแนนเสียงแบบอิเล็กทรอนิกส์โดยใช้ บล็อกเชนแบบส่วนตัว

**นักศึกษา** นายกานต์ เนียมจันทร์ รหัสนักศึกษา 57070004

นายอภิชัย ตันตสิรินทร์ รหัสนักศึกษา 57070142

**ปริญญา** วิทยาศาสตร์บัณฑิต

**สาขาวิชา** เทคโนโลยีสารสนเทศ

**ปีการศึกษา** 2560

**อาจารย์ที่ปรึกษา** ผศ.ดร.ปานวิทย์ ธุวะนุติ

# บทคัดย่อ

ในปัจจุบันการเลือกตั้งหรือการลงคะแนนเสียงแบบเดิมที่ใช้กันทั่วไปนั้นยังไม่สามารถพิสูจน์ได้ว่ามีความโปร่งใสจริงหรือไม่ เนื่องจากมีการเก็บเป็นเอกสารใส่ในอุปกรณ์บรรจุที่ไม่ได้รับรองความปลอดภัยได้อย่างชัดเจนและข้อมูลนั้นเป็นเอกสารที่อาจจะเกิดความเสียหายทำให้ข้อมูลทั้งหมดผิดพลาดไป อีกทั้งยังเป็นการสิ้นเปลืองทรัพยากรขององค์กรในการจัดทำอุปกรณ์เก็บผลลงคะแนนเสียงและการจัดทำบัตรลงคะแนน

โครงงานฉบับนี้จึงจัดทำขึ้นเพื่อสร้างความมั่นใจว่าการลงคะแนนเสียงของผู้มีสิทธิลงคะแนนทุกคนจะได้รับความปลอดภัยและไม่ถูกเปลี่ยนแปลง โดยใช้เทคโนโลยี Blockchain ที่มีความปลอดภัยสูงและเป็นที่ยอมรับอย่างแพร่หลายในปัจจุบัน ระบบนี้สามารถนำไปใช้ในการลงคะแนนเสียงภายในองค์กร เพื่อเพิ่มประสิทธิภาพความปลอดภัยและความโปร่งใสในการลงคะแนน

**Project Title**  Electronic Vote By Private Blockchain

**Student** Mr. Karn Niamchan Student ID 57070004

Mr. Apichai Tantasirin Student ID 57070142

**Degree** Bachelor of Science

**Program** Information Technology

**Academic Year** 2017

**Advisor**  Assistant Professor Dr. Panwit Tuwanut

# ABSTRACT

In the current election or traditional voting cannot prove that is transparent or not. Because keeping a document in the ballot box does not guarantee a security clearly. And the document may be corrupt, make all the wrong information. It is also a waste of corporate resources, in the preparation of the storage and preparation of the voting ballots. This project is purpose to make confidence of voting will be safety and cannot be changed with Blockchain technology that is highly secure and can be accepted. This system can be applied to a vote within the organization. To enhance security and transparency in the voting.

# กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สามารถสำเร็จสมบูรณ์ได้ด้วยความกรุณาของผู้ช่วยศาสตราจารย์ ดร.ปานวิทย์ ธุวะนุติ อาจารย์ที่ปรึกษาปริญญานิพนธ์ ที่ให้คำปรึกษาคำแนะนำต่าง ๆ แนวคิดการออกแบบตลอดจนแก้ไขปัญหาที่เกิดขึ้นตลอดการพัฒนา ด้วยความเอาใจใส่อย่างดียิ่งทางผู้จัดทำจึงขอกราบขอบพระคุณอย่างสูง

นอกจากนี้ยังขอขอบคุณอาจารย์ทุกท่านในคณะเทคโนโลยีสารสนเทศ ที่ให้ความรู้ คำปรึกษาและชี้แนะแนวทางต่าง ๆ ซึ่งสามารถนำมาใช้ประโยชน์ในการแก้ปัญหาและนำความรู้ไปต่อยอดในอนาคต

ขอขอบคุณเพื่อนๆพี่ๆในคณะเทคโนโลยีสารสนเทศและผู้ที่มีส่วนเกี่ยวข้องที่ได้ให้คำปรึกษาและความช่วยเหลือมาโดยตลอด

สุดท้ายนี้ผู้จัดทำขอขอบคุณบิดา มารดา และครอบครัวที่คอยสนับสนุนเป็นกำลังใจ ให้คำปรึกษาและความช่วยเหลือในทุก ๆ ด้าน จนทำให้ปริญญานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี

กานต์ เนียมจันทร์

อภิชัย ตันตสิรินทร์

สารบัญ

หน้า

[บทคัดย่อ I](#_Toc513046879)

[ABSTRACT II](#_Toc513046880)

[กิตติกรรมประกาศ III](#_Toc513046881)

[สารบัญรูป VIII](#_Toc513046882)

[สารบัญรูป (ต่อ) IX](#_Toc513046883)

[บทที่ 1 1](#_Toc513046884)

[บทนำ 1](#_Toc513046885)

[1.1 ความเป็นมาและความสำคัญของงานวิจัย 1](#_Toc513046886)

[1.2 วัตถุประสงค์ของโครงงานพัฒนาระบบ 1](#_Toc513046887)

[1.3 ขอบเขตของงานวิจัย 2](#_Toc513046888)

[1.4 ขั้นตอนและวิธีการดำเนินการศึกษาโครงการ 2](#_Toc513046889)

[1.5 ประโยชน์ที่คาดว่าจะได้รับ 3](#_Toc513046890)

[บทที่ 2 4](#_Toc513046891)

[แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง 4](#_Toc513046892)

[2.1 Blockchain 4](#_Toc513046893)

[2.2 User Interface Design 6](#_Toc513046894)

[2.3 Web application 9](#_Toc513046895)

[2.4 ภาษาแอชทีเอ็มแอล (HTML) 10](#_Toc513046896)

[2.5 ซีเอสเอส (CSS) 10](#_Toc513046897)

[2.6 ภาษาจาวาสคริปท์ (JavaScript) 11](#_Toc513046898)

[2.7 มาตราฐานความปลอดภัยของการลงคะแนนเสียง 12](#_Toc513046899)

[2.8 Data Encryption 12](#_Toc513046900)

[2.9 Ethereum blockchain 13](#_Toc513046901)

[2.10 Solidity 14](#_Toc513046902)

[2.11 Node.js 14](#_Toc513046903)

[บทที่ 3 15](#_Toc513046904)

[การวิเคราะห์และออกแบบระบบ 15](#_Toc513046905)

[3.1 การวิเคราะห์และศึกษาระบบงานแบบเดิม 15](#_Toc513046906)

[3.2 ปัญหาที่พบเห็นในระบบปัจจุบัน 15](#_Toc513046907)

[3.3 วิเคราะห์ความต้องการ 16](#_Toc513046908)

[3.4 การออกแบบระบบใหม่ 16](#_Toc513046909)

[บทที่ 4 30](#_Toc513046910)

[4.1 ส่วนที่ติดต่อกับผู้จัดตั้งการลงคะแนนเสียง 30](#_Toc513046911)

[4.2 ส่วนที่ติดต่อกับผู้ลงคะแนนเสียง 35](#_Toc513046912)

[4.3 ผลการทดลองเชื่อมต่อ Blockchain เบื้องต้น 38](#_Toc513046913)

[บทที่ 5 44](#_Toc513046914)

[5.1 สรุปผลการดำเนินงาน 44](#_Toc513046915)

[5.2 ปัญหาและอุปสรรคที่พบ 45](#_Toc513046916)

[5.3 ข้อจำกัดของระบบ 45](#_Toc513046917)

[บรรณานุกรม 47](#_Toc513046918)

**สารบัญตาราง**

ตารางที่ หน้า

[3.1 แสดง Use Case Description สร้างแบบฟอร์มการลงคะแนนเสียง............................................17](#_ตารางที่_3.1_รายละเอียดการทำงานของฟ)

[3.2 แสดง Use Case Description ข้อมูลการลงคะแนนเสียงและจำนวนผู้ที่ลงคะแนน....................18](#_ตารางที่_3.2_รายละเอียดการทำงานของฟ)

[3.3 แสดง Use Case Description แสดงผลการลงคะแนนเสียงทั้งหมด...........................................19](#_ตารางที่_3.3_รายละเอียดการทำงานของฟ)

[3.4 แสดง Use Case Description ตรวจสอบและยืนยันชื่อผู้ที่มาลงคะแนนเสียง.............................20](#_ตารางที่_3.4_รายละเอียดการทำงานของฟ)

[3.5 แสดง Use Case Description การเข้าสู่ระบบ.............................................................................21](#_ตารางที่_3.5_รายละเอียดการทำงานของฟ)

[3.6 แสดง Use Case Description ผู้เข้าร่วมลงคะแนนทำการลงคะแนนเสียง..................................22](#_ตารางที่_3.6_รายละเอียดการทำงานของฟ)

# สารบัญรูป

รูปที่ หน้า

บทที่ 2

[*รูปที่* 2.1 *ความแตกต่างระหว่าง* Proof-of-Work *กับ* Proof-of-Stake 5](#_Toc512814084)

[*รูปที่* 2.2 *ตัวอย่างเทคโนโลยีปัญญาประดิษฐ์* Siri *ของ* Apple 6](#_Toc512814085)

[รูปที่ 2.3 ตัวอย่าง terminal prompt ใน mac 7](#_Toc512814086)

[รูปที่ 2.4 ตัวอย่าง dashboard on macOS 8](#_Toc512814087)

[รูปที่ 2.5 ตัวอย่างการทำงานของเว็บแอปพลิเคชัน 9](#_Toc512814088)

[รูปที่ 2.6 สัญลักษณ์ HTML 10](#_Toc512814089)

[รูปที่ 2.7 สัญลักษณ์ CSS 10](#_Toc512814090)

[รูปที่ 2.8 สัญลักษณ์ JavaScript 11](#_Toc512814091)

[รูปที่ 2.9 การเข้ารหัสแบบ Symmetric key 12](#_Toc512814092)

[รูปที่ 2.10 การเข้ารหัสแบบ Asymmetric key 13](#_Toc512814093)

[รูปที่ 2.11 สัญลักษณ์ Solidity 14](#_Toc512814094)

บทที่ 3

[รูปที่ 3.1โครงสร้างของระบบ 16](#_Toc512814141)

[รูปที่ 3.2 แผนภาพยูสเคส (Use Case Diagram) 17](#_Toc512814142)

[รูปที่ 3.3 แสดงแผนภาพกิจกรรมการเข้าสู่ระบบ 24](#_Toc512814143)

[รูปที่ 3.4 แสดงแผนภาพกิจกรรมการสร้างฟอร์มลงคะแนนเสียง 25](#_Toc512814144)

[รูปที่ 3.5 แสดงแผนภาพตรวจสอบและยืนยันชื่อผู้ที่มาลงคะแนนเสียง 26](#_Toc512814145)

[รูปที่ 3.6 แสดงแผนภาพการแสดงผลข้อมูลโดยรวม 27](#_Toc512814146)

[รูปที่ 3.7 แสดงแผนภาพการลงคะแนนเสียงโดยผู้ลงคะแนนเสียง 28](#_Toc512814147)

[รูปที่ 3.8 แสดงแผนภาพการแสดงผลสรุปการลงคะแนนเสียง 29](#_Toc512814148)

บทที่ 4

[รูปที่ 4.1 หน้าแรกของระบบ 30](#_Toc512814223)

[รูปที่ 4.2 หน้าเข้าสู่ระบบ 31](#_Toc512814224)

[รูปที่ 4.3 หน้าสร้างการลงคะแนนของผู้จัดตั้งการลงคะแนนเสียง 31](#_Toc512814225)

[รูปที่ 4.4 หน้าอัพโหลดรูปภาพของหัวข้อหรือตัวเลือก 32](#_Toc512814226)

[รูปที่ 4.5 หน้าตรวจสอบและยืนยันชื่อผู้ที่มาลงคะแนนเสียงของผู้จัดการลงคะแนนเสียง 33](#_Toc512814227)

# สารบัญรูป (ต่อ)

รูปที่ หน้า

[รูปที่ 4.6 หน้าแสดงระบบยืนยันตนผู้เข้าร่วมโหวตสร้างรหัสขึ้นมาให้ 33](#_Toc512814228)

[รูปที่ 4.7 หน้าแสดงข้อมูลการลงคะแนนเสียงและจำนวนผู้ที่ลงคะแนนเสียง 34](#_Toc512814229)

[รูปที่ 4.8 หน้าแสดงผลคะแนนการโหวตทั้งหมด 34](#_Toc512814230)

[รูปที่ 4.9 หน้าลงคะแนนเสียงของผู้ลงคะแนน 35](#_Toc512814231)

[รูปที่ 4.10 ผู้ลงคะแนนใช้สิทธิ์ลงคะแนนเสียงของตนเอง 36](#_Toc512814232)

[รูปที่ 4.11 การลงคะแนนเสียงสำเร็จ 36](#_Toc512814233)

[รูปที่ 4.12 หน้าแสดงผลการลงคะแนนเสียงทั้งหมด 37](#_Toc512814234)

[รูปที่ 4.13 แสดงการเขียนพารามิเตอร์ในไฟล์ genesis.json 38](#_Toc512814235)

[รูปที่ 4.14 แสดงคำสั่งการ Initialization ด้วยไฟล์ genesis.json ที่ได้สร้างขึ้น 38](#_Toc512814236)

[รูปที่ 4.15 แสดงผลลัพธ์จากการพิมคำสั่ง Initialization ไฟล์ genesis.json 39](#_Toc512814237)

[รูปที่ 4.16 แสดงผลลัพธ์จากการพิมคำสั่งของ geth เพื่อเข้าสู่ console 39](#_Toc512814238)

[รูปที่ 4.17 แสดงผลลัพธ์จากการใช้คำสั่ง admin.nodeInfo 39](#_Toc512814239)

[รูปที่ 4.18 แสดงผลลัพธ์จากการใช้คำสั่ง personal.newAccount() 40](#_Toc512814240)

[รูปที่ 4.19 แสดงการเขียนพารามิเตอร์ในไฟล์ genesis.json 40](#_Toc512814241)

[รูปที่ 4.20 แสดงคำสั่งการ Initialization ด้วยไฟล์ genesis.json 40](#_Toc512814242)

[รูปที่ 4.21 แสดงคำสั่งและแสดงผลลัพธ์ เพื่อเข้าสู่ console 41](#_Toc512814243)

[รูปที่ 4.22 แสดงผลลัพธ์จองการใช้คำสั่ง admin.nodeInfo 41](#_Toc512814244)

[รูปที่ 4.23 แสดงผลลัพธ์จากการใช้คำสั่ง personal.newAccount() 41](#_Toc512814245)

[รูปที่ 4.24 แสดงการใช้คำสั่งเพื่อเชื่อมต่อระหว่างคอมพิวเตอร์ 42](#_Toc512814246)

[รูปที่ 4.25แสดงผลลัพธ์จากคอมพิวเตอร์เครื่องที่ 2 โดยใช้คำสั่ง admin.peers 42](#_Toc512814247)

[รูปที่ 4.26 แสดงผลลัพธ์จากคอมพิวเตอร์เครื่องที่ 1 โดยใช้คำสั่ง admin.peers 42](#_Toc512814248)

[รูปที่ 4.27 แสดงผลลัพธ์จากคอมพิวเตอร์เครื่องที่ 1 โดยใช้คำสั่ง eth.blockNumber 43](#_Toc512814249)

[รูปที่ 4.28 แสดงผลลัพธ์จากคอมพิวเตอร์เครื่องที่ 2 โดยใช้คำสั่ง eth.blockNumber 43](#_Toc512814250)

# บทที่ 1

### บทนำ

## 1.1 ความเป็นมาและความสำคัญของงานวิจัย

นับแต่แรกเริ่มของระบบระบอบประชาธิปไตย การเลือกตั้งต่าง ๆทั่วโลกมักถูกมองว่าไม่มีความโปร่งใส และในยุคที่เทคโนโลยีเข้ามามีผลกระทบต่อชีวิตประจำวันก็เริ่มมีการปรับปรุงประสิทธิภาพของกระบวนการเลือกตั้งออนไลน์อย่างแพร่หลาย แต่ก็ยังมีกลุ่มคนบางส่วนที่ยังไม่เห็นด้วยในระบบนี้เนื่องจากระบบการเลือกตั้งแบบดั้งเดิมนั้นเป็นระบบที่ตรวจสอบได้ยากขาดความโปร่งใสและความไม่เสถียรของระบบการเลือกตั้ง การที่เราใช้เทคโนโลยีขั้นสูงนี้จะทำให้สามารถเพิ่มประสิทธิภาพและความโปร่งใสในการเลือกตั้งโดยไม่ส่งผลกระทบต่อความเป็นส่วนตัวของผู้มีสิทธิเลือกตั้งและมีหลักการในการพิสูจน์ว่า ผลการเลือกตั้งมีความถูกต้อง นอกจากนี้ผู้มีสิทธิ์เลือกตั้งจะสามารถร้องขอดูคะแนนเสียงของตนได้เพื่อให้มั่นใจวาการลงคะแนนเสียงของตนได้รับการเก็บรักษาอย่างปลอดภัยและตรวจสอบว่ามีการเปลี่ยนแปลงใด ๆ หรือไม่ โดยปกติเมื่อมีการนำเทคโนโลยีใหม่ๆเข้ามา จะมีค่าใช้จ่ายที่สูงขึ้นเพื่อใช้ประโยชน์จากเทคโนโลยีใหม่ๆการเพิ่มจำนวนผู้มีสิทธิ์เลือกตั้งจะเป็นผลประโยชน์จากการนำเทคโนโลยีการเลือกตั้งออนไลน์อย่างปลอดภัย ความจริงในอดีตมีหลายบริษัทที่พยายามจะเป็นเจ้าภาพในการจัดการเลือกตั้งออนไลน์แต่ก็ต้อหล้มเหลวไป เนื่องจากวิธีการทางเทคโนโลยีที่ใช้ไม่สามารถรับรองได้ว่ามีความปลอดภัยของข้อมูล หากเราสามารถเอาชนะความเข้าใจผิดว่าการลงคะแนนเสียงอิเล็กทรอนิกส์ไม่สามารถทำได้อย่างปลอดภัย เราจะสามารถกระตุ้นคนยุคใหม่ที่มีสิทธิ์เลือกตั้งมาคะแนนเสียงอิเล็กทรอนิกส์ได้จากทุกที่บนโลกตอนนี้เรามีเทคโนโลยีที่จะทำให้ทุกอย่างเป็นไปได้ สิ่งที่เราต้องการจากคุณคือการสนับสนุนของคุณเพื่อทำให้เป็นจริง

## 1.2 วัตถุประสงค์ของโครงงานพัฒนาระบบ

1. เพื่อศึกษาหลักการทำงานของระบบบล็อคเชน (blockchain) และนำไปประยุกต์ใช้กับบล็อกเชนแบบส่วนบุคคล (private blockchain)

2. เพื่อเพิ่มความปลอดภัยและความถูกต้องของการลงคะแนน สามารถตรวจสอบได้ว่าข้อมูลที่ได้มานั้นไม่มีการเปลี่ยนแปลงโดยใช้การเข้ารหัส

3. เพื่อให้มั่นใจว่าผลของการลงคะแนนมีความถูกต้องและเป็นไปอย่างโปร่งใส

## 1.3 ขอบเขตของงานวิจัย

ระบบนี้จะเป็นระบบที่ช่วยเพิ่มความปลอดภัยในการเก็บรักษาข้อมูลโดยระบบถูกออกแบบมาให้มีหน้าที่หลักการทำงานดังนี้

1. พัฒนาระบบในรูปแบบ เว็บแอปพลิเคชัน (Web Application)

2. ประยุกต์ใช้บล็อกเชนแบบส่วนบุคคลเป็นฐานข้อมูลจัดการและตรวจสอบความถูกต้องของข้อมูลแบบกระจาย

ระบบจะแบ่งออกเป็น 2 ส่วนคือ

1.) ส่วนผู้จัดตั้งการลงคะแนนเสียง

2.) ส่วนของผู้ลงคะแนนเสียง

โดยผู้จัดตั้งการลงคะแนนเสียงสามารถกำหนดสิทธิ์ให้ผู้ลงคะแนนได้ว่าใครมีสิทธิ์ลงคะแนนได้ในส่วนของผู้ลงคะแนนสามารถลงคะแนนเสียงได้อย่างเดียว

## 1.4 ขั้นตอนและวิธีการดำเนินการศึกษาโครงการ

1. ศึกษาหลักการทำงานของบล็อคเชน (blockchain) แบบบล็อคเชนแบบส่วนบุคคล (private blockchain) สำหรับการประยุกต์ใช้เพื่อระบบลงคะแนนเสียง

2. ศึกษาการเข้ารหัสของข้อมูล (Data Encryption)

3. ศึกษาวิธีการสร้างเว็บแอปพลิเคชัน (Web Application)

4. ออกแบบระบบการลงคะแนน แบ่งออกเป็น 2 ส่วน

1.) การวางระบบบล็อกเชนแบบส่วนบุคคล

2.) พัฒนาเว็บแอปพลิเคชันสำหรับการลงคะแนนเสียง

1.4.5 พัฒนาระบบให้เป็นไปตามขอบเขตของงาน

1.4.6 ทดสอบระบบและปรับปรุงระบบให้พร้อมใช้งาน

## 1.5 ประโยชน์ที่คาดว่าจะได้รับ

ระบบการลงคะแนนเสียงแบบอิเล็กทรอนิกส์ช่วยสนับสนุนการทำงานและอำนวยประโยชน์ดังนี้

1. ความปลอดภัยของข้อมูลการลงแนนในระบบ

2. ข้อมูลของการลงคะแนนจะมีความถูกต้องและไม่สามารถแก้ไขได้

3. มีความโปร่งใสเพิ่มมากขึ้นในการจัดตั้งการลงคะแนน

4. ลดการใช้กระดาษเนื่องจากมีการใช้เว็บแอปพลิเคชันแทน

# บทที่ 2

### แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

## 2.1 Blockchain

เทคโนโลยีบล็อคเชนคือ ระบบการจัดเก็บข้อมูลแบบกระจายโดยเป็นการเก็บไว้ในเครื่องของผู้ใช้งานโดยทุกคนสามารถเข้าถึงและได้รับข้อมูลเดียวกันทำให้รู้ว่าผู้ใดมีสิทธิและเป็นเจ้าของข้อมูลจริง ๆ โดยสามารถบันทึกธุรกรรมจำนวนมากได้เช่นการทำธุรกรรมทางการเงินหรือแม้แต่การเก็บบัตรลงคะแนนเสียงการทำธุรกรรมทั้งหมดที่เกิดขึ้นในบล็อคเชนแบบมาตรฐานจะได้รับการตรวจสอบและเซ็นชื่อด้วยการเข้ารหัสเพื่อความปลอดภัย [1]

#### 2.1.1 แรงจูงใจในการใช้บล็อคเชน

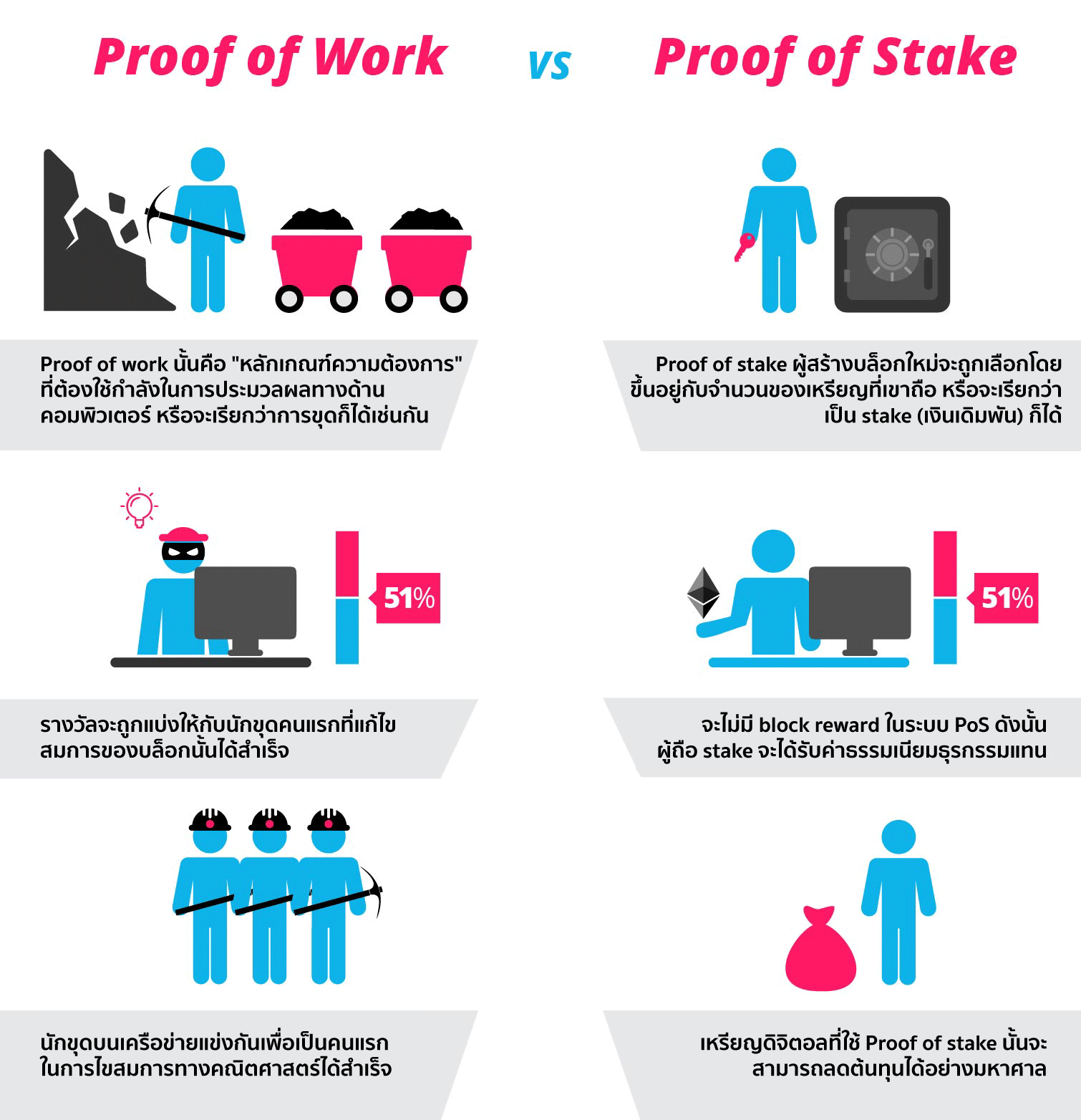
เนื่องจากฐานข้อมูลแบบดั้งเดิมจะถูกเก็บรักษาโดยองค์กรเดียวและองค์กรดังกล่าวมีอำนาจในการควบคุมฐานข้อมูลรวมถึงความสามารถในเก็บรักษาข้อมูลและสามารถเปลี่ยนแปลงหรือแก้ไขข้อมูลได้ซึ่งถือเป็นความไม่ปลอดภัยต่อข้อมูลสำหรับกรณีการใช้งานส่วนใหญ่ปัญหานี้ไม่ใช่ปัญหาเนื่องจากองค์กรที่ดูแลรักษาฐานข้อมูลทำเพื่อประโยชน์ของตนเองและไม่มีเหตุผลที่จะทำให้เนื้อหาของฐานข้อมูลถูกปลอมแปลง อย่างไรก็ตามมีกรณีการใช้งานอื่น ๆ เช่น เครือข่ายทางการเงินซึ่งเป็นข้อมูลที่มีความอ่อนไหวมากซึ่งมีความเสี่ยงมากเพื่อให้องค์กรเดียวสามารถควบคุมฐานข้อมูลทั้งหมด แม้ว่าจะสามารถรับประกันได้ว่าองค์กรที่รับผิดชอบจะไม่เปลี่ยนแปลงข้อมูลภายในฐานข้อมูล ก็ยังมีความเป็นไปได้ที่แฮ็กเกอร์จะเจาะเข้าฐานข้อมูลและจัดการเปลี่ยนแปลงหรือปลอมแปลงข้อมูล วิธีที่ดีที่สุดเพื่อให้มั่นใจว่าไม่มีใครที่สามารถจัดการกับฐานข้อมูลได้คือการทำให้ฐานข้อมูลเป็นแบบสาธารณะและอนุญาตให้ทุกคนเก็บสำเนาของฐานข้อมูลที่ซ้ำซ้อน ด้วยวิธีนี้ทุกคนสามารถมั่นใจได้ว่าสำเนาฐานข้อมูลของตนมีความสมบูรณ์เพียงแค่เปรียบเทียบกับฐานข้อมูลของคนอื่นเท่าที่ฐานข้อมูลยังไม่ถูกเปลี่ยนแปลง แต่ถ้าฐานข้อมูลถูกเปลี่ยนแปลงหลังจากที่ทุกคนเก็บสำเนาฐานข้อมูลเก่าไปแล้วปัญหาของฉันทามติจึงเกิดขึ้น

#### 2.1.2 เทคโนโลยีบล็อคเชนทำงานอย่างไร ?

เทคโนโลยีบล็อคเชนสามารถแก้ไขปัญหาได้โดยการสร้างเครือข่ายคอมพิวเตอร์ (nodes) มีหน้าที่หลักๆ 2 อย่างคือควบคุมและป้องกันการซ้ำของข้อมูลโดยบล็อกเชนถูกควบคุมด้วยกฎฉันทามติ (Blockchain Consensus Protocol) ซึ่งประเภทของโปรโตคอลฉันทามติมี 2 ประเภทหลัก

1.) Proof-of-work เป็นโปรโตคอลหรือชุดคำสั่ง ปัจจุบันมีการใช้งานโดย Bitcoin (ณ เดือนมกราคม 2016) และ Blockchains อื่น ๆ อีกมากมาย หลักการทำงานคือการตรวจสอบการทำธุรกรรมที่ถูกนำมารวมกันไว้และเก็บไว้ในบล็อคซึ่งจะต้องใช้เครื่องคอมพิวเตอร์เข้ามาช่วย (Miner) ด้วยวิธีการแก้ไขสมการทางคณิตศาสตร์โดยจะมอบรางวัลให้กับ Miner แรกที่ทำการไขสมการได้สำเร็จ จะได้รับรางวัลตอบแทนจากนั้นบล็อคเก็บธุรกรรมที่ถูกตรวจสอบจะนำไปเก็บไว้ใน Blockchain

2.) Proof-of-stake เป็นโปรโตคอลที่ใช้ในการตรวจสอบธุรกรรมอีกหนึ่งวิธีแต่มีขั้นตอนและวิธีการที่แตกต่างจาก Proof-of-work คือการสร้างบล็อคใหม่นั้นจะถูกควบคุมโดย stake ที่มีจำนวนเงินในครอบครองจะนำเงินมาวางเป็นทุน ทำให้มีความสามารถในการยืนยันธุรกรรมได้ เมื่อการยืนยันธุรกรรมเสร็จสิ้นทุนนั้นก็จะคืนสู่เจ้าของพร้อมกับเงินจำนวนเล็กน้อยที่เป็นค่าธุรกรรม



*รูปที่* 2.1 *ความแตกต่างระหว่าง* Proof-of-Work *กับ* Proof-of-Stake [2]

โดยกลุ่มของการทำธุรกรรมที่ถูกเพิ่มทั้งหมดโดยโหนดนั้นเรียกว่า บล็อค แต่ละบล็อคจะมีการอ้างอิงถึงบล็อคก่อนหน้าซึ่งจะกำหนดลำดับของบล็อคจึงเป็นจุดเริ่มต้นของคำว่า "Blockchain" โดยเป็นห่วงโซ่ของแต่ละบล็อคที่จะเชื่อมต่อไปยังบล็อคก่อนหน้ากับรายการธุรกรรมใหม่ๆ เมื่อมีโหนดใหม่จะเข้าร่วมเครือข่ายจะเริ่มต้นด้วยฐานข้อมูลว่างและดาวน์โหลดบล็อคทั้งหมดโดยใช้ธุรกรรมภายในฐานข้อมูลเพื่อส่งต่อฐานข้อมูลจากโหนดใหม่ไปยังสถานะเดียวกับโหนดอื่น ๆ ทั้งหมด โดยพื้นฐานแล้วบล็อคเชนจะกำหนดลำดับการทำธุรกรรมกับฐานข้อมูลเพื่อให้ทุกคนสามารถตรวจสอบได้ว่ามีความถูกต้องและยืนยันว่าไม่มีการเปลี่ยนแปลงที่ไม่เหมาะสม

## 2.2 User Interface Design

การออกแบบส่วนต่อประสานกับผู้ใช้ ระหว่างผู้ใช้กับคอมพิวเตอร์ให้ผู้ใช้สามารถเข้าใจรูปแบบการใช้งานระบบทำความเข้าใจได้ง่าย

รูปแบบของ UI มี 3 แบบหลัก ๆ คือ

#### 2.2.1 การโต้ตอบด้วยภาษามนุษย์ (Natural Language Interaction : NLI)

เทคโนโลยีด้านปัญญาประดิษฐ์ (Artificial Intelligent: AI) ใช้ input ด้วยภาษามนุษย์โดยการพูดหรือการพิม เช่น Siri (Apple), Cortana (Microsoft) เป็นต้น



*รูปที่* 2.2 *ตัวอย่างเทคโนโลยีปัญญาประดิษฐ์* Siri *ของ* Apple

**ข้อดี**

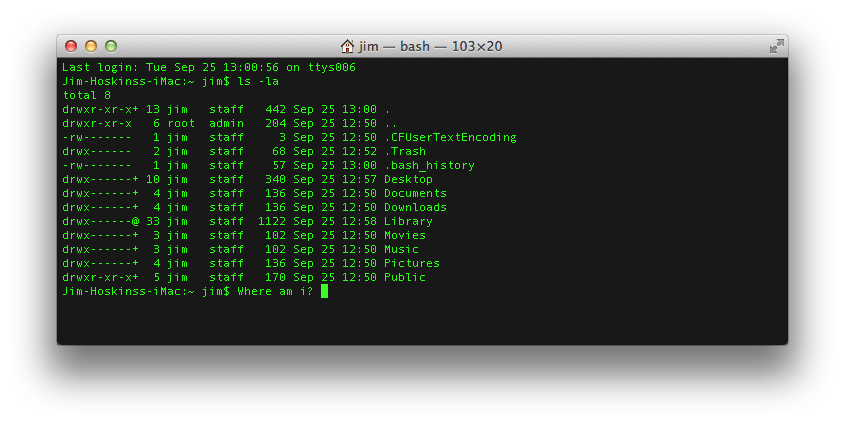
* ใช้งานง่าย ไม่ซับซ้อน
* ผู้ใช้งานทุกประเภท สามารถใช้งานได้

**ข้อเสีย**

* ต้องการเทคโนโลยีขั้นสูงในการพัฒนา

#### 2.2.2 การโต้ตอบด้วยคำสั่ง (Command Language Interaction : CLI)

การโต้ตอบด้วยคำสั่ง เป็นการป้อนคำสั่งเป็นตัวอักษร ผ่านคีย์บอร์ดเป็นอุปกรณ์ input เข้าสู่ระบบและแสดงออกเป็นตัวอักษร ผ่านทางหน้าจอ โดยแต่ละระบบปฏิบัติการก็จะมี cli เป็นของตัวเอง คำสั่งที่ใช้ใน cli ของแต่ละระบบปฏิบัติการก็จะแตกต่างกันออกไปและมีชื่อเรียกตัว cli ที่แตกต่างกันออกไป เช่น Microsoft จะเรียกว่า Command Prompt (CMD), Apple จะเรียกว่า Terminal Prompt



รูปที่ 2.3 ตัวอย่าง terminal prompt ใน mac

**ข้อดี**

* มีการประมวลผลที่รวมเร็ว
* ใช้งานง่าย ไม่ซับซ้อน

**ข้อเสีย**

* ต้องใช้คำสั่งเฉพาะของแต่ละระบบนั้นๆ
* รูปแบบการใช้งานไม่เป็นมิตรกับผู้ใช้ทั่วไป

#### 2.2.3 การโต้ตอบด้วยกราฟฟิค (Graphics User Interaction : GUI)

การโต้ตอบด้วยกราฟฟิค เป็นการใช้งานระบบที่เข้าใจได้ง่ายที่สุดเพราะ ผู้ใช้งานจะเข้าใจระบบได้ผ่านรูปภาพหรือวัตถุ ที่สามารถมองเห็น ได้ยิน หรือสัมผัสได้



รูปที่ 2.4 ตัวอย่าง dashboard on macOS

**ข้อดี**

* ใช้งานง่าย ไม่ซับซ้อน
* รูปแบบสวยงาม น่าใช้งาน
* เป็นภาษาสากลที่เป็นเชิงสัญลักษณ์

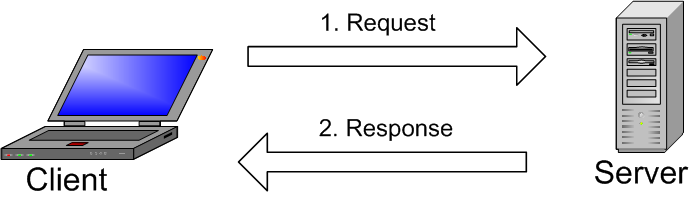
**ข้อเสีย**

* ออกแบบยาก
* ทำงานได้ช้าในเครื่องที่มีสเปคต่ำ

## 2.3 Web application

เว็บแอปพลิเคชัน คือ โปรแกรมที่ถูกสร้างขึ้นเพื่อสนับสนุนการทำงานของระบบสารสนเทศต่าง ๆ สามารถเรียกใช้งานผ่านทางเว็บบราวเซอร์ โดยอาศัยโปรโตคอล HTTPS

การทำงานของเว็บแอปพลิเคชัน จะแบ่งออกเป็น 2 ฝั่งหลัก ๆ คือ



รูปที่ 2.5 ตัวอย่างการทำงานของเว็บแอปพลิเคชัน

#### 2.3.1 Client หรือเรียกว่าฝั่งผู้ใช้งาน ประกอบไปด้วย 3 ส่วนหลัก

1.) เว็บเบราว์เซอร์ (Web Browser) เป็นซอฟต์แวร์ที่ผู้ใช้เข้าถึงเว็บแอปพลิเคชัน โดยผู้ใช้งานจะต้องทราบและใส่ที่อยู่เว็บไซต์ที่ต้องการใช้งาน เช่น ใส่ที่อยู่เว็บไซต์ https://www.facebook.com เว็บเบราว์เซอร์ก็จะทำการสร้าง HTTP request เพื่อส่งคำร้องไปยังเว็บเซิร์ฟเวอร์ผ่านเครือข่ายบนอินเตอร์เน็ต และเมื่อคำร้องไปถึงเว็บเซิร์ฟเวอร์ เว็บเซิร์ฟเวอร์ก็จะส่ง HTTP response ตอบกลับมาที่ client และแสดงผลผ่านเว็บเบราว์เซอร์

2.) ส่วนเสริมความสามารถของเว็บเบราว์เซอร์ (Plugin) คือโปรแกรมที่ถูกสร้างขึ้นมาให้ทำงานร่วมกับเว็บเบราว์เซอร์ได้เพื่อเพิ่มประสิทธิภาพของเว็บเบราว์เซอร์ เช่น Adobe Flash, PDF reader

3.) ระบบปฏิบัติการ (Operating System) ระบบปฏิบัติการเป็นตัวกลางระหว่างผู้ใช้และคอมพิวเตอร์มีหน้าที่บริหารจัดการทรัพยากรภายในเครื่องคอมพิวเตอร์ ในส่วนของ web application ระบบปฏิบัติการทำหน้าที่ในการรับ HTTP request จากเบราว์เซอร์และส่งเข้าสู่อินเตอร์เน็ตและยังมีหน้าที่แปลง URL ให้เป็น IP Address เพื่อค้นหาที่อยู่ปลายทางของที่อยู่นั้น ๆ

#### 2.3.2 Server หรือเรียกว่าฝั่งเซิร์ฟเวอร์

เว็บแอปพลิเคชั่น (Web Application) ทำหน้าที่ติดต่อกับผู้ใช้งาน รับข้อมูลเข้า ประมวลผลข้อมูล จัดการข้อมูลต่าง ๆ ในฐานข้อมูล และแสดงผลข้อมูลได้ เว็บแอปพลิเคชันสามารถแบ่งออกได้เป็น 3 ส่วนคือ

1.) ส่วนติดต่อกับผู้ใช้งานเพื่อรับและแสดงผลข้อมูล (View)

2.) ส่วนประมวลผลการทำงาน (Controller)

3.) ส่วนที่ใช้ในการติดต่อและจัดการกับข้อมูลและฐานข้อมูล (Model)

เว็บเซิร์ฟเวอร์ซอฟต์แวร์ (Web Server Software) เป็นโปรแกรมที่ทำงานอยู่บนเว็บเซิร์ฟเวอร์ หน้าที่หลักของเว็บเซิร์ฟเวอร์คือการประมวลผล HTTP request จาก client ที่ส่งเข้ามาและคอยตอบกลับด้วย HTTP response

## 2.4 ภาษาแอชทีเอ็มแอล (HTML)

****

รูปที่ 2. สัญลักษณ์ HTML

HTML ย่อมาจาก Hypertext Markup Language คือ ภาษาที่ออกแบบมาเพื่อใช้เขียนโครงสร้างเว็บไซต์ โดยมีตัวกำกับ (tag) ควบคุมการแสดงผลของข้อความ ตาราง แบบฟอร์ม รูปภาพอื่น ๆ ที่สามารถแสดงผลผ่านเว็บเบราว์เซอร์ได้ ตัวอย่างของ tag เช่น <head>, <title>, <body>, <article>, <section>, <p>, <div>, <span>, <img>

HTML เริ่มพัฒนาโดย ทิม เบอร์เนอรส์ ลี (Tim Berners Lee) ในปัจจุบัน HTML ถูกจัดเป็นมาตรฐานหนึ่งใน ISO ซึ่งมีองค์กรณ์ที่ชื่อว่า World Wide Web Consortium (W3C)

## 2.5 ซีเอสเอส (CSS)

****

รูปที่ 2.7 สัญลักษณ์ CSS

Cascading Style Sheets (CSS) เป็นภาษา Stylesheet Language ใช้เพื่ออธิบายการนำเสนอเอกสารที่เขียนในรูปแบบ HTML หรือ XML เพื่อเป็นการตกแต่งหรือจัดการองค์ประกอบเพื่อที่จะแสดงผลบนหน้าจอ หรือสื่ออื่น ๆ ได้อย่างสวยงาม

## 2.6 ภาษาจาวาสคริปท์ (JavaScript)

****

รูปที่ 2.8 สัญลักษณ์ JavaScript

JavaScript คือ ภาษาคอมพิวเตอร์สาหรับการเขียนโปรแกรมบนระบบอินเทอร์เน็ต และ เป็นที่รู้จัก กันดีในฐานะภาษาสคริปต์สำหรับเว็บเพจ ซึ่งมีวิธีการทางานในลักษณะ “แปลความและดำเนินงานไปทีละคำสั่ง (interpret)” หรือเรียกว่า อ็อบเจ็กโอเรียลเต็ด (Object Oriented Programming) จาวาสคริปต์ทำงานบน JavaScript เป็นภาษาสคริปต์ที่มีประสิทธิภาพใช้กันอย่างแพร่หลายในการควบคุมพฤติกรรมของ หน้าเว็บ

## 2.7 มาตราฐานความปลอดภัยของการลงคะแนนเสียง

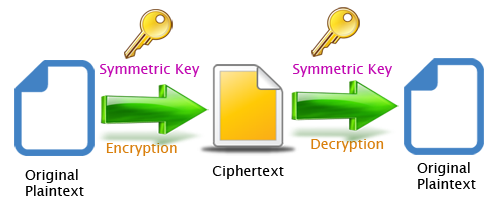
การลงคะแนนเสียงแบบคอมพิวเตอร์จะไม่ถูกนำมาใช้สำหรับการลงคะแนนเสียงเว้นแต่จะมีโปรโตคอลที่รักษาความเป็นส่วนตัวของแต่ละบุคคลและป้องกันการโกง ต้องมีข้อกำหนดอย่างน้อย 6 ข้อสำหรับการจะนำมาใช้งาน

1. ผู้มีสิทธิเท่านั้นที่จะสามาระลงคะแนนเสียงได้
2. ไม่มีใครสามารถลงคะแนนได้มากกว่า 1 ครั้ง
3. ไม่มีใครสามารถตัดสินได้ว่าใครสามารถลงคะแนนได้บ้าง
4. ไม่มีใครสามารถคัดลอกคะแนนของผู้อื่นได้ (เป็นความต้องการที่ยากที่สุด)
5. ไม่มีใครเปลี่ยนแปลงคะแนนเสียงของผู้อื่นได้โดยไม่ถูกค้นพบ
6. ผู้มีสิทธิลงคะแนนเสียงทุกคนสามารถตรวจสอบได้ว่า การลงคะแนนเสียงของตนถูกนำมาพิจารณา
7. ทุกคนสามารถรู้ได้ว่าใครโหวตหรือไม่โหวต

## 2.8 Data Encryption

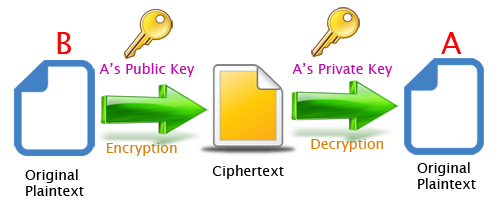
เป็นเทคโนโลยีการเข้ารหัสข้อมูลวิธีการหนึ่งของการรักษาความปลอดภัยของข้อมูล ไม่ให้ข้อมูลถูกอ่านได้โดยบุคคลอื่น หลักการของการเข้ารหัสข้อมูลคือแปลงข้อมูลให้อยู่ในรูปที่ไม่สามารถอ่านได้โดยตรง (encryption) หากต้องการอ่านข้อมูลจะต้องทำการถอดรหัส (Decryption) ก่อนซึ่งจะได้ผลลัพธ์เป็นข้อมูลดั้งเดิมก่อนทำการเข้ารหัส โดยการเข้ารหัสจะแบ่งออกเป็น 2 ประเภทใหญ่ๆคือ

1.) Symmetric Cryptography (Secret key) เป็นการเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสตัวเดียวกัน คือ ผู้รับและผู้ส่งจะต้องมีกุญแจรหัสที่เหมือนกันเพื่อใช้ในการเข้ารหัสหรือถอดรหัส



รูปที่ 2.9 การเข้ารหัสแบบ Symmetric key

2.) Asymmetric Cryptography (Public Key) เป็นการเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสคนละตัวกัน คือ ทั้งผู้รับและผู้ส่งจะมีกุญแจรหัสคนละ 2 ตัวเสมอคือกุญแจสาธารณะ (public key) และกุญแจส่วนตัว (private key) โดยมีหลักการทำงานคือ หาเข้ารหัสด้วยกุญแจใดจะต้องถอดรหัสด้วยกุญแจอีกตัวเป็นคู่กัน



รูปที่ 2.10 การเข้ารหัสแบบ Asymmetric key

## 2.9 Ethereum blockchain

Ethereum เป็นแพลตฟอร์มแบบเปิดของ Blockchain ที่ทำให้ทุกคนสามารถสร้างและใช้งานแอปพลิเคชันแบบกระจายข้อมูล (decentralized) ซึ่งทำงานบนเทคโนโลยี Blockchain ได้ Ethereum มีความคล้าย Bitcoin ตรงที่ไม่มีใครสามารถควบคุมหรือเป็นเจ้าของ Ethereum ได้ เนื่องจาก Ethereum เป็นโครงการแบบโอเพนซอร์ส (open-source project) ที่สร้างขึ้นโดยผู้คนเป็นจำนวนมากจากทั่วโลก แต่ Ethereum มีความแตกต่างจากโปรโตคอล Bitcoin เนื่องจาก Ethereum ถูกออกแบบมาเพื่อให้สามารถปรับตัวได้และมีความยืดหยุ่น การสร้างแอ็พพลิเคชันใหม่ ๆ บนแพลตฟอร์ม Ethereum เป็นเรื่องง่าย และสามารถใช้งานแอปพลิเคชันเหล่านี้ได้อย่างปลอดภัย มีสัญญาอัจฉริยะ(Smart Contract) ที่ทำงานอยู่บน Ethereum ไว้ติดต่อกับบล็อกเชนทำให้สามารถใช้ในการบันทึกข้อตกลงของสัญญาที่สามารถดำเนินการได้ด้วยตัวเองโดยไม่จำเป็นต้องมีคนกลางหรือคนมาคอยตรวจสอบ

## 2.10 Solidity

Solidity คือ ภาษาคอมพิวเตอร์สำหรับเขียนโปรแกรมที่ใช้สำหรับเขียนสัญญาอัจฉริยะ (Smart Contract) บน Ethereum เพื่อดึงข้อมูลหรือเก็บข้อมูลลง Blockchainโดย Solidity นั้น มีพื้นฐานมาจาก Java Script



รูปที่ 2.11 สัญลักษณ์ Solidity

## 2.11 Node.js

Node.js คือ Cross Platform Runtime Environment สำหรับฝั่ง Server และเป็น Open source ซึ่งเขียนด้วยภาษา JavaScript มีการทำงานเป็น Asynchronous คือ การทำงานบางอย่างไม่ต้องรอให้บรรทัดนั้นทำงานเสร็จ

# บทที่ 3

### การวิเคราะห์และออกแบบระบบ

## 3.1 การวิเคราะห์และศึกษาระบบงานแบบเดิม

การลงคะแนนเสียงแบบเดิมนั้นจะมีขั้นตอนดังนี้

1. ตรวจสอบสิทธิในการลงคะแนนเสียงของตนเอง
2. ยื่นหลักฐานแสดงตนและลงลายมือตัวเองให้กับเจ้าหน้าที่รับ
3. รับบัตรลงคะแนน
4. ไปยังจุดคูหาลงคะแนนเสียงที่เจ้าหน้าที่เตรียมไว้ให้ และทำการลงคะแนนเสียงโดยทำเครื่องหมาย X ลงในช่องที่ต้องการลงคะแนนเสียง
5. เดินไปยังจุดส่งคะแนนเสียง และหย่อนคะแนนเสียงลงไปด้วยตัวเอง

เมื่อหมดเวลาลงคะแนนเสียง เจ้าหน้าที่ควบคุมการลงคะแนนเสียงจะเปิดหีบใส่คะแนนและเก็บไว้อย่างดีและจะมีการตรวจสอบจำนวนของบัตรลงคะแนนว่าตรงกับจำนวนเอกสารยืนยันตนกับที่มีผู้มาลงทะเบียนใช้สิทธิลงคะแนนหรือไม่ ถ้าเกิดเหตุการณ์ที่นับจำนวนบัตรกับจำนวนเอกสารยืนยันตนไม่เท่ากัน จะทำให้เกิดการเปิดให้ลงคะแนนเสียงใหม่ และเมื่อเอกสารและจำนวนบัตรตรงกันแล้วก็จะทำการนับคะแนนโดยมีการจัดสถานที่นับและประกาศคะแนนเสียงซึ่งจะต้องกระทำโดยเป็นการเปิดเผยต่อผู้ลงคะแนนเสียงได้เห็นและรับรู้ และต้องนับบัตรคะแนนเสียงทุกใบที่อยู่ในหีบลงคะแนนเสียงเท่านั้น

## 3.2 ปัญหาที่พบเห็นในระบบปัจจุบัน

1. การรับบัตรลงคะแนนเสียงที่เป็นกระดาษ และมีการผลิตหีบเก็บผลลงคะแนน ซึ่งเป็นการสิ้นเปลืองงบประมาณ
2. ไม่สามารถตรวจสอบได้อย่างแน่ชัดว่าการเก็บคะแนนเสียงก่อนนำไปนับคะแนนนั้นจะไม่มีการทุจริตกันเกิดขึ้น
3. ความปลอดภัยในการเก็บข้อมูลผลลงคะแนนเสียง เนื่องจากข้อมูลเป็นแบบเอกสารกระดาษเมื่อเกิดเหตุการณ์ที่ไม่คาดคิด เช่น ไฟไหม้ จะทำให้ข้อมูลลงคะแนนเสียงเสียหายได้

## 3.3 วิเคราะห์ความต้องการ

ความต้องการที่เป็นหน้าที่หลักของระบบ (Functional Requirement )

* ผู้ลงคะแนนเสียงสามารถลงคะแนนเสียงผ่านระบบที่จัดเตรียมไว้
* ข้อมูลการโหวตของผู้ใช้งานจะไม่ตรวจสอบได้ว่าโหวตไหนเป็นของใคร
* ข้อมูลการโหวตจะไม่สามารถแก้ไขได้หลังจากทำการลงคะแนนเสียง

ความต้องการที่ไม่เป็นหน้าที่หลักของระบบ (Non-Functional Requirement)

* การออกแบบที่ทำให้เข้าใจได้ง่าย ใช้งานง่าย

## 3.4 การออกแบบระบบใหม่

#### 3.4.1 ผลการออกแบบโครงสร้างระบบ

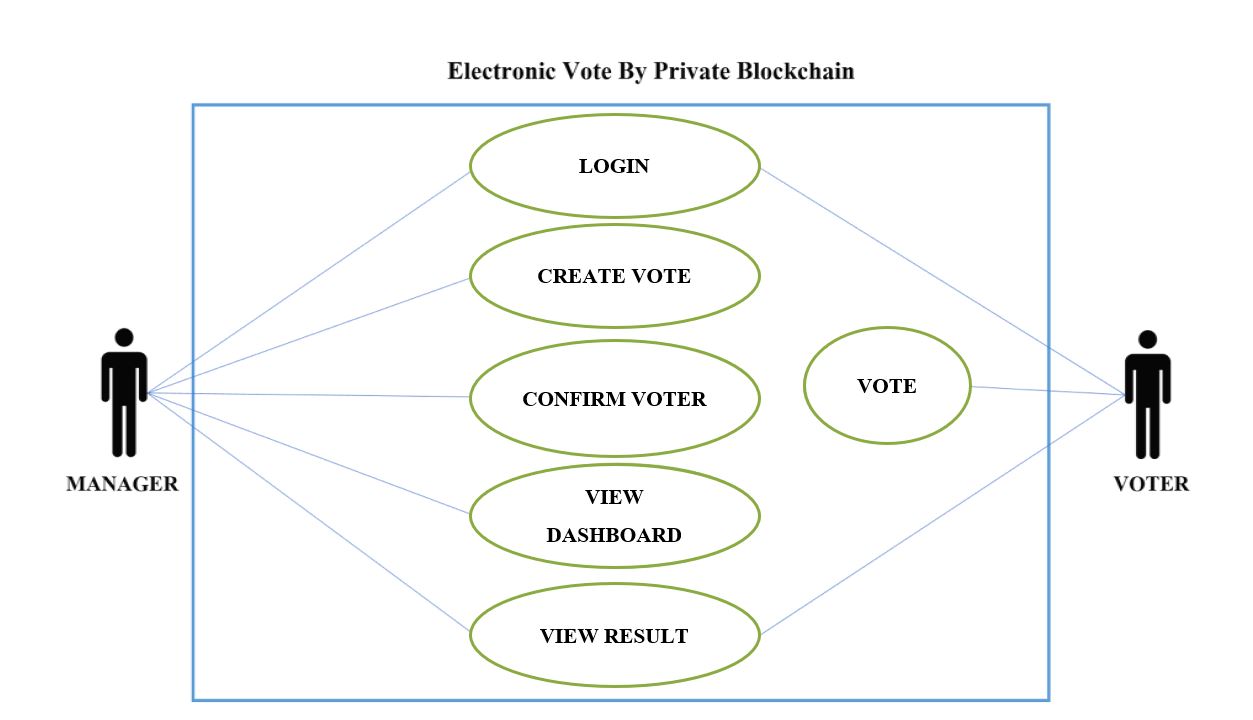
กระบวนการของระบบการลงคะแนนเสียงอิเล็กทรอนิกส์ ขั้นแรกผู้มีสิทธิ์ลงคะแนนเสียงจะถูกเข้ารหัสคะแนนเสียงด้วยกุญแจสาธารณะ ( public key ) ของผู้จัดการเลือกตั้ง ต่อมาคะแนนเสียงที่ถูกเข้ารหัสอยู่จะถูกลงนามโดยใช้กุญแจส่วนตัว ( private key ) ของผู้มีสิทธิ์ลงคะแนน การลงนามและการเข้ารหัสจะถูกเก็บลงฐานข้อมูล ในฐานข้อมูล ID ของผู้มีสิทธิ์ลงคะแนนเสียงจะได้รับการตรวจสอบด้วยการยืนยันลายเซ็นของคะแนนเสียงที่ถูกเข้ารหัส จากนั้นลายเซ็นจะถูกลบออกจากคะแนนเสียงที่เข้ารหัสและถูกส่งไปถอดรหัสคะแนนเสียงโดยใช้กุญแจส่วนตัวของผู้จัดการเลือกตั้งแล้วนับคะแนนดังภาพที่ 3.1



รูปที่ 3.1โครงสร้างของระบบ

#### 3.4.2 แผนภาพยูสเคส (Use Case Diagram)

เป็นแผนภาพที่แสดงถึงรายละเอียดว่ามีผู้ใช้ที่เกี่ยวข้องกับระบบนี้มีใครบ้าง และมีกิจกรรมอะไรบ้าง ซึ่งมีรายละเอียดดังนี้



รูปที่ 3.2 แผนภาพยูสเคส (Use Case Diagram)

ผู้ที่เกี่ยวข้องในระบบ (Actor) ประกอบด้วย

* Manager
* Voter

**องค์ประกอบของ Use Case**

ส่วนของผู้จัดการโหวต

1. Login
2. Create vote
3. Confirm voter
4. View dashboard
5. View result

ส่วนของผู้ลงคะแนนเสียง

1. Login
2. Vote
3. View result

#### 3.4.3 ตารางแสดงรายละเอียดของฟังก์ชั่นการทำงาน (Use case description)

###### **ตารางที่** 3.1 รายละเอียดการทำงานของฟังก์ชั่น สร้างแบบฟอร์มการลงคะแนนเสียง

|  |  |  |
| --- | --- | --- |
| Use case name | Create vote | ID : 1 |
| Scenario | สร้างแบบฟอร์มการลงคะแนนเสียง | |
| Triggering event | - | |
| Brief description | ผู้จัดตั้งการลงคะแนนเสียงทำการสร้างฟอร์มการลงคะแนนเสียง โดยมีการระบุหัวข้อโหวต ตัวเลือกโหวต ช่วงเวลาโหวต และจำนวนคนลงคะแนนเสียง | |
| Actors | Manager | |
| Related use case | - | |
| Pre-condition | - | |
| Post-condition | View dashboard | |
| Flow of actvities | Actor | System |
|  | 1. 1. สร้างการโหวตและระบุช่วงเวลาในการโหวต | 2.สร้างการลงคะแนนเสียงบนเว็บ |
| Exception conditions | - | |

###### **ตารางที่** 3.2 รายละเอียดการทำงานของฟังก์ชั่น ดูข้อมูลการลงคะแนนเสียงและจำนวนผู้ที่ลงคะแนน

|  |  |  |
| --- | --- | --- |
| Use case name | View dashboard | ID : 2 |
| Scenario | ข้อมูลการลงคะแนนเสียงและจำนวนผู้ที่ลงคะแนน | |
| Triggering event | - | |
| Brief description | ผู้จัดตั้งการลงคะแนนดูจำนวนผู้ที่ลงคะแนนเสียงแล้ว | |
| Actors | Manager | |
| Related use case | Create vote | |
| Pre-condition | Create vote | |
| Post-condition | - | |
| Flow of actvities | Actor | System |
|  | 1. 1. ผู้จัดตั้งการลงคะแนนดูจำนวนผู้ที่ลงคะแนนเสียงแล้ว | 1. 2. ระบบจะตรวจสอบจำนวนผู้ที่ลงคะแนนเสียง แล้วนำมาแสดงผล |
| Exception conditions |  | |

###### **ตารางที่** 3.3 รายละเอียดการทำงานของฟังก์ชั่น แสดงผลการลงคะแนนเสียงทั้งหมด

|  |  |  |
| --- | --- | --- |
| Use case name | View result | ID : 3 |
| Scenario | แสดงผลการลงคะแนนเสียงทั้งหมด | |
| Triggering event | - | |
| Brief description | หน้าจอแสดงผลการลงคะแนนเสียงทั้งหมด | |
| Actors | Manager, User | |
| Related use case | Create vote, Vote | |
| Pre-condition | Vote | |
| Post-condition | - | |
| Flow of actvities | Actor | System |
|  | 1. 1. ผู้จัดตั้งการลงคะแนนและ   ผู้ลงคะแนนดูผลสรุปการลงคะแนนเสียงทั้งหมด | 1. 2. ระบบจะนำข้อมูลที่ถูกถอดรหัสมานับและแสดงผล |
| Exception conditions |  | |

###### **ตารางที่** 3.4 รายละเอียดการทำงานของฟังก์ชั่น ตรวจสอบและยืนยันชื่อผู้ที่มาลงคะแนนเสียง

|  |  |  |
| --- | --- | --- |
| Use case name | Confirm voter | ID : 4 |
| Scenario | ตรวจสอบและยืนยันชื่อผู้ที่มาลงคะแนนเสียง | |
| Triggering event | - | |
| Brief description | ตรวจสอบและยืนยันชื่อผู้ที่มาลงคะแนนเสียง | |
| Actors | Manager | |
| Related use case | - | |
| Pre-condition | - | |
| Post-condition | - | |
| Flow of actvities | Actor | System |
|  | 1. 1. ผู้จัดตั้งการลงคะแนนตรวจสอบและเพิ่มผู้ลงคะแนนลงฐานข้อมูล | 1. 2. ระบบจะทำการเพิ่มข้อมูลของผู้ลงคะแนนลงฐานข้อมูล |
| Exception conditions |  | |

###### **ตารางที่** 3.5 รายละเอียดการทำงานของฟังก์ชั่น ผู้จัดตั้งการลงคะแนนเสียงหรือผู้ลงคะแนนเสียงทำการเข้าสู่ระบบ

|  |  |  |
| --- | --- | --- |
| Use case name | Login | ID : 5 |
| Scenario | ผู้จัดตั้งการลงคะแนนเสียงหรือผู้ลงคะแนนเสียงทำการเข้าสู่ระบบ | |
| Triggering event | - | |
| Brief description | ผู้จัดตั้งการลงคะแนนเสียงหรือผู้ลงคะแนนเสียงทำการกรอกข้อมูลเพื่อเข้าสู่ระบบ | |
| Actors | User, Manager | |
| Related use case | Vote | |
| Pre-condition | Confirm voter | |
| Post-condition |  | |
| Flow of actvities | Actor | System |
|  | 1. 1. ผู้จัดตั้งการลงคะแนนเสียงหรือผู้ลงคะแนนเสียงกรอกข้อมูลเพื่อเข้าสู่ระบบ 2. 2. กดปุ่ม Login |  |
| Exception conditions | ผู้จัดตั้งการลงคะแนนเสียงหรือผู้ลงคะแนนเสียงกรอกรหัสผิดหรือกรอกไม่ครบถ้วน | |

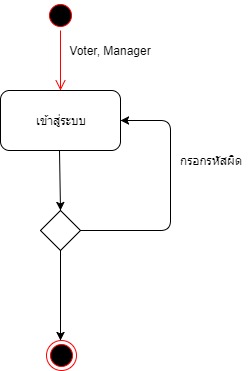
###### **ตารางที่** 3.6 รายละเอียดการทำงานของฟังก์ชั่น ผู้เข้าร่วมลงคะแนนทำการลงคะแนนเสียง

|  |  |  |
| --- | --- | --- |
| Use case name | Vote | ID : 6 |
| Scenario | ผู้เข้าร่วมลงคะแนนทำการลงคะแนนเสียง | |
| Triggering event | - | |
| Brief description | ผู้เข้าร่วมลงคะแนนทำการลงคะแนนเสียง | |
| Actors | Voter | |
| Related use case |  | |
| Pre-condition | Login | |
| Post-condition |  | |
| Flow of actvities | Actor | System |
|  | 1. 1. ผู้เข้าร่วมลงคะแนนทำการลงคะแนนเสียง | 1. 2. ทำการเข้ารหัสข้อมูลการลงคะแนนและเก็บเข้าสู่ฐานข้อมูลบล็อคเชน |
| Exception conditions |  | |

#### 3.4.4 แผนภาพกิจกรรม (Activities Diagram)

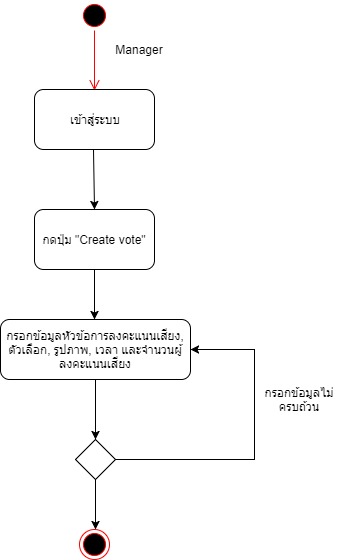
แผนภาพกิจกรรม(Activities Diagram) คือแผนภาพที่ใช้แสดงให้เห็นถึงลำดับขั้นตอนการทำงานของระบบในกระบวนการของแต่ละฟังก์ชั่น

Activities Diagram: เข้าสู่ระบบ



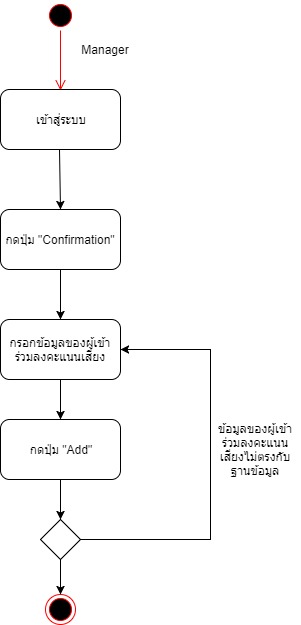
รูปที่ 3.3 แสดงแผนภาพกิจกรรมการเข้าสู่ระบบ

Activities Diagram: สร้างแบบฟอร์มการลงคะแนนเสียง



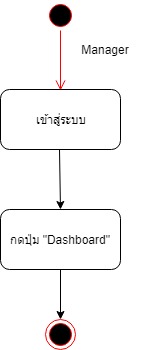
รูปที่ 3.4 แสดงแผนภาพกิจกรรมการสร้างฟอร์มลงคะแนนเสียง

Activities Diagram: ตรวจสอบและยืนยันชื่อผู้ที่มาลงคะแนนเสียง



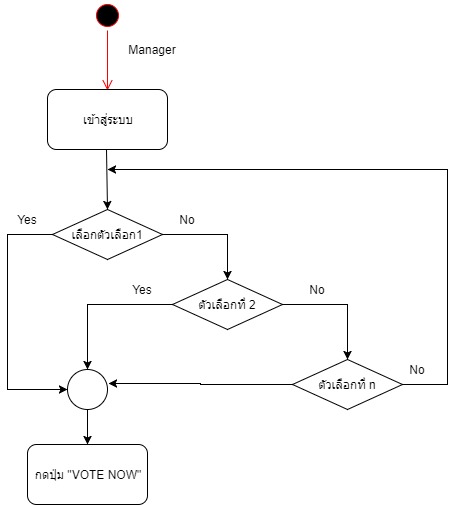
รูปที่ 3.5 แสดงแผนภาพตรวจสอบและยืนยันชื่อผู้ที่มาลงคะแนนเสียง

Activities Diagram: View dashboard



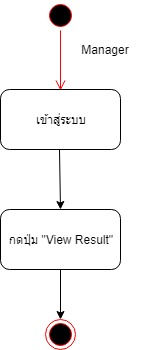
รูปที่ 3.6 แสดงแผนภาพการแสดงผลข้อมูลโดยรวม

Activities Diagram: Vote



รูปที่ 3.7 แสดงแผนภาพการลงคะแนนเสียงโดยผู้ลงคะแนนเสียง

Activities Diagram: View result



รูปที่ 3.8 แสดงแผนภาพการแสดงผลสรุปการลงคะแนนเสียง

# บทที่ 4

**ระบบต้นแบบ**

การพัฒนาระบบต้นแบบตามที่ผู้ศึกษาได้ดำเนินการศึกษาและออกแบบไว้จะนำเสนอในรูปแบบของ Web Application ซึ่งรองรับการใช้งานทุกแพลตฟอร์มโดยแบ่งการพัฒนาออกเป็นดังนี้

## 4.1 ส่วนที่ติดต่อกับผู้จัดตั้งการลงคะแนนเสียง

#### 4.1.1 หน้าแรก

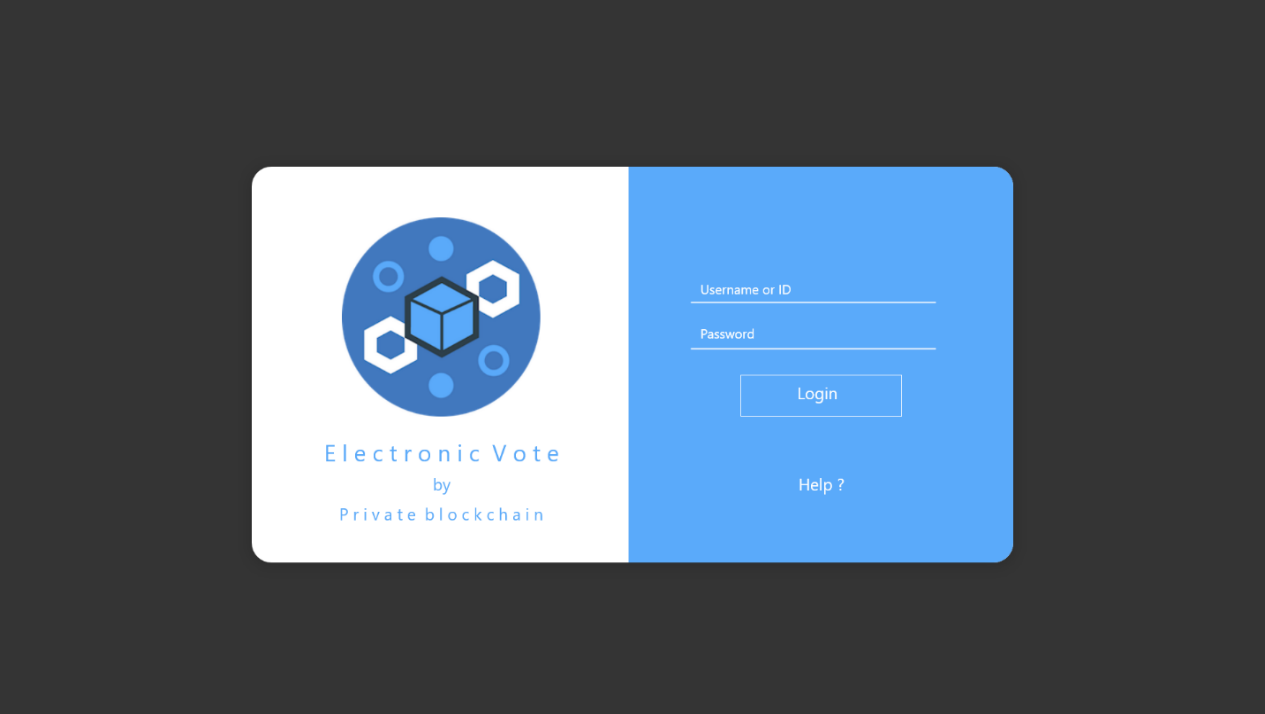
หน้าที่แสดงถึงโครงสร้างพื้นฐานและอธิบายเกี่ยวกับเทคโนโลยีบล็อคเชนที่ทางผู้พัฒนามีการนำมาใช้ว่ามีความปลอดภัยและโปร่งใส



รูปที่ 4.1 หน้าแรกของระบบ

#### 4.1.2 หน้าเข้าสู่ระบบ

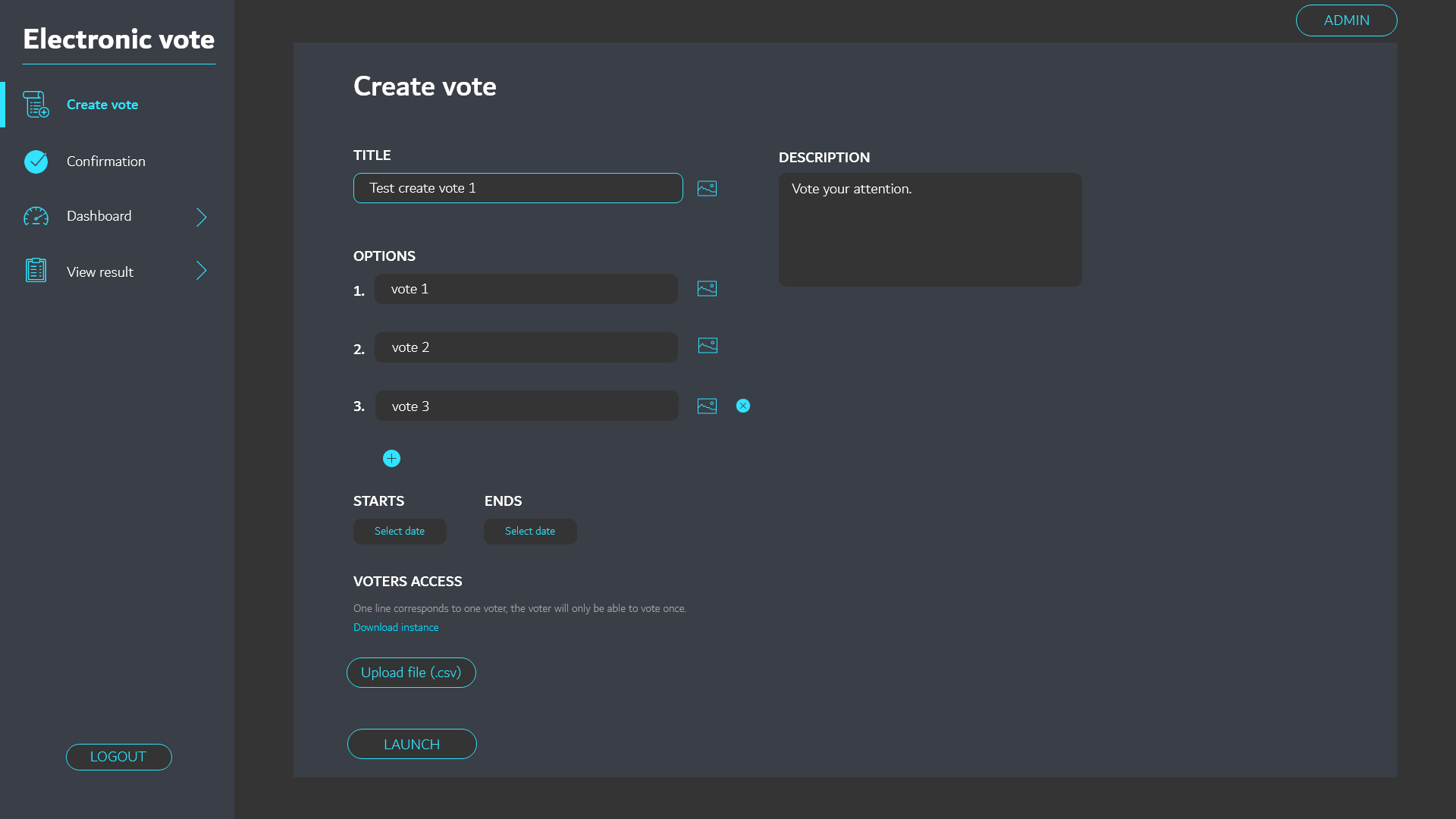
แสดงหน้าการเข้าสู่ระบบของผู้จัดตั้งการลงคะแนนเสียงและผู้ลงคะแนนเสียง โดยผู้จัดตั้งการลงคะแนนเสียงจะต้องกรอก username และ password ให้ถูกต้อง หลังจากนั้นระบบจะพาไปยังหน้าสร้างการลงคะแนนของผู้จัดการลงคะแนนเสียงดังรูปที่ 3 หรือผู้ลงคะแนนเสียงต้องกรอก ID กับ password ที่ได้มาเพื่อไปยังหน้าลงคะแนนเสียงดังรูปที่ 9



รูปที่ 4.2 หน้าเข้าสู่ระบบ

#### 4.1.3 หน้าสร้างการลงคะแนนของผู้จัดตั้งการลงคะแนนเสียง

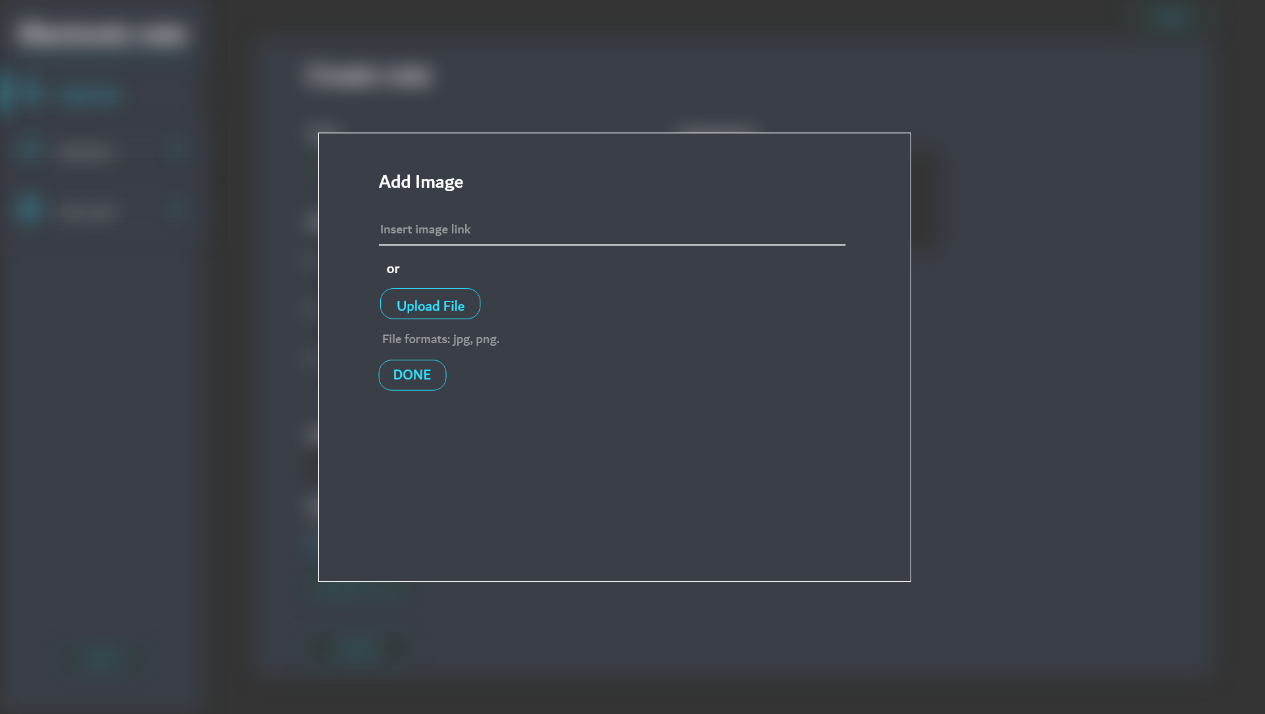
ในหน้านี้ผู้จัดตั้งการลงคะแนนเสียงจะต้องกรอกข้อมูลได้แก่ หัวข้อของการลงคะแนน ตัวเลือกในการลงคะแนนสามารถเพิ่มหรือลดจำนวนตัวเลือกได้โดยสามารถใส่รูปภาพได้ดังรูป 4.4 ต้องกำหนดระยะเวลาเริ่มให้ผู้ลงคะแนนเสียงสามารถลงคะแนนได้ และระยะเวลาที่ปิดระบบ และทำการ upload file excel ที่มีข้อมูลชื่อ-นามสกุลกับเลขบัตรประจำตัวประชาชนของผู้มีสิทธิ์ลงคะแนน เมื่อกรอกข้อมูลเสร็จสิ้นให้คลิกที่ปุ่ม “LAUNCH” เพื่อเริ่มทำการสร้างโหวต



รูปที่ 4.3 หน้าสร้างการลงคะแนนของผู้จัดตั้งการลงคะแนนเสียง

#### 4.1.4 หน้าอัพโหลดรูปภาพของหัวข้อหรือตัวเลือก

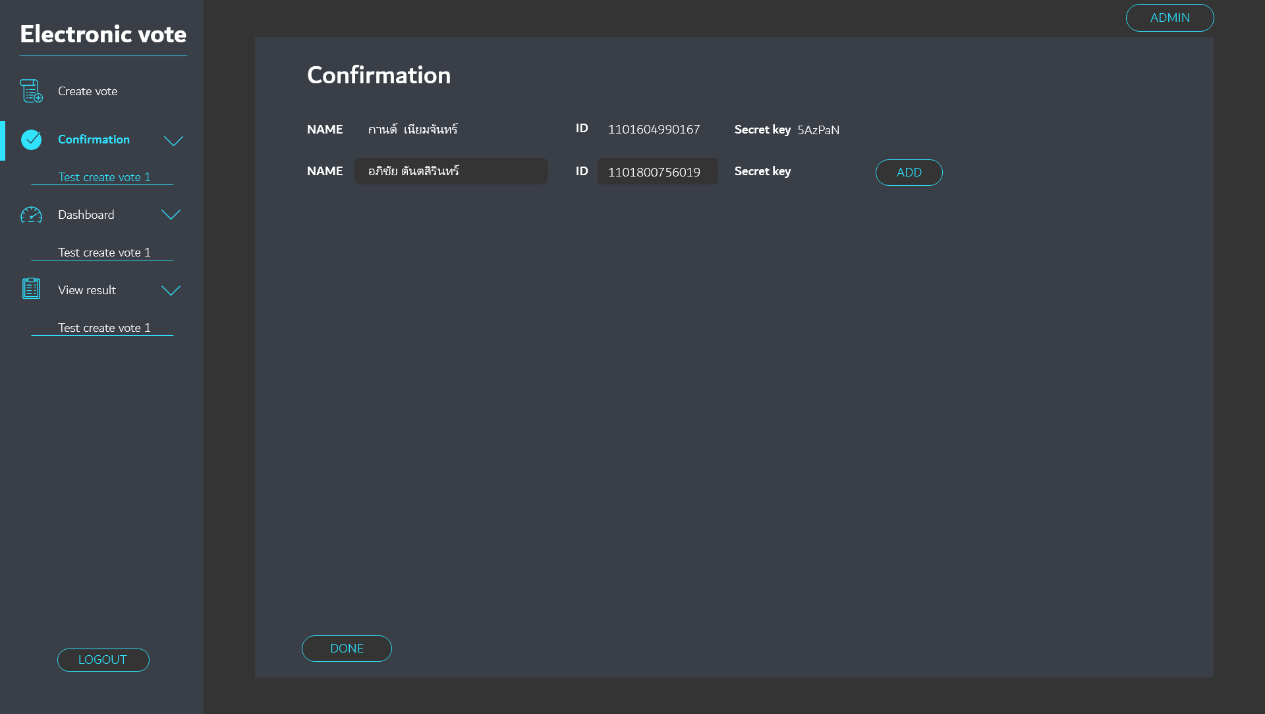
ในหน้านี้สามารถอัพโหลดรูปหรือใส่ลิ้งของรูปภาพ



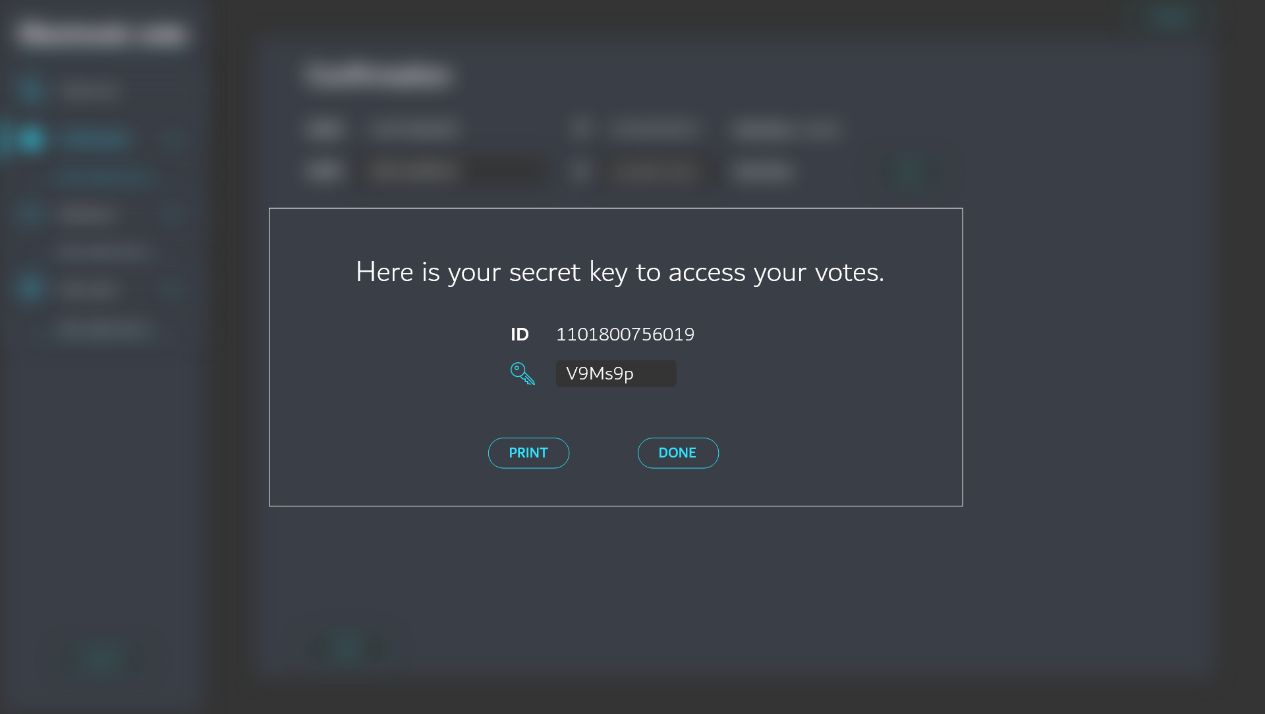
รูปที่ 4.4 หน้าอัพโหลดรูปภาพของหัวข้อหรือตัวเลือก

#### 4.1.5 หน้าตรวจสอบและยืนยันชื่อผู้ที่มาลงคะแนนเสียงของผู้จัดการลงคะแนนเสียง

ในหน้านี้จะแสดงถึงรายชื่อและเลขบัตรประจำตัวประชาชนของผู้ที่มาเข้าร่วมลงคะแนนแล้วและมีช่องให้กรอกชื่อเพื่อยืนยันตัวตน โดยระบบจะนำไปเช็คกับฐานข้อมูลถ้าชื่อที่กรอกตรงกับฐานข้อมูลระบบจะทำการสร้างรหัสให้ดังรูป 6 เพื่อนำไปใช้ Login เข้าสู่การลงคะแนนเสียง



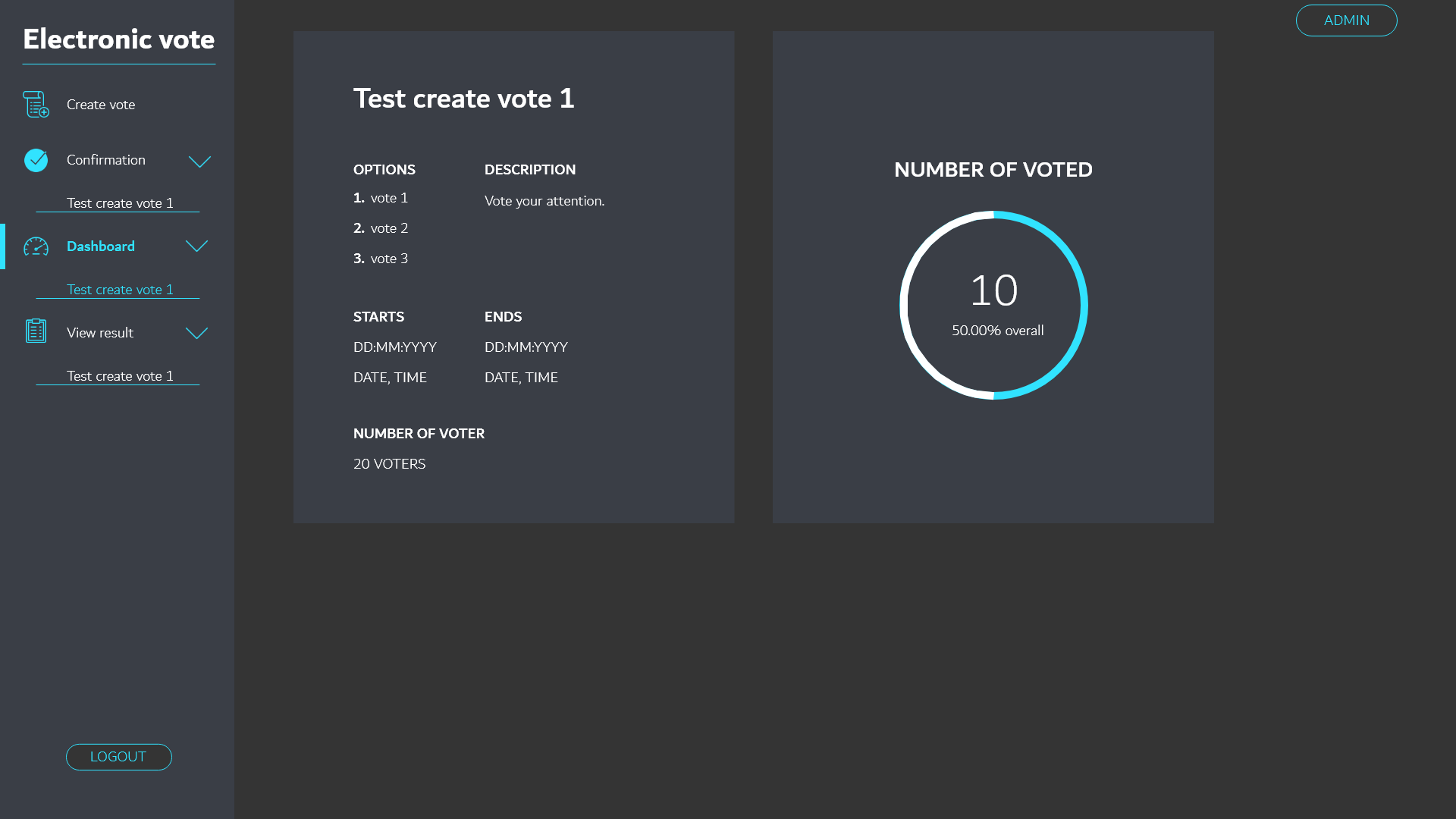
รูปที่ 4.5 หน้าตรวจสอบและยืนยันชื่อผู้ที่มาลงคะแนนเสียงของผู้จัดการลงคะแนนเสียง



รูปที่ 4.6 หน้าแสดงระบบยืนยันตนผู้เข้าร่วมโหวตสร้างรหัสขึ้นมาให้

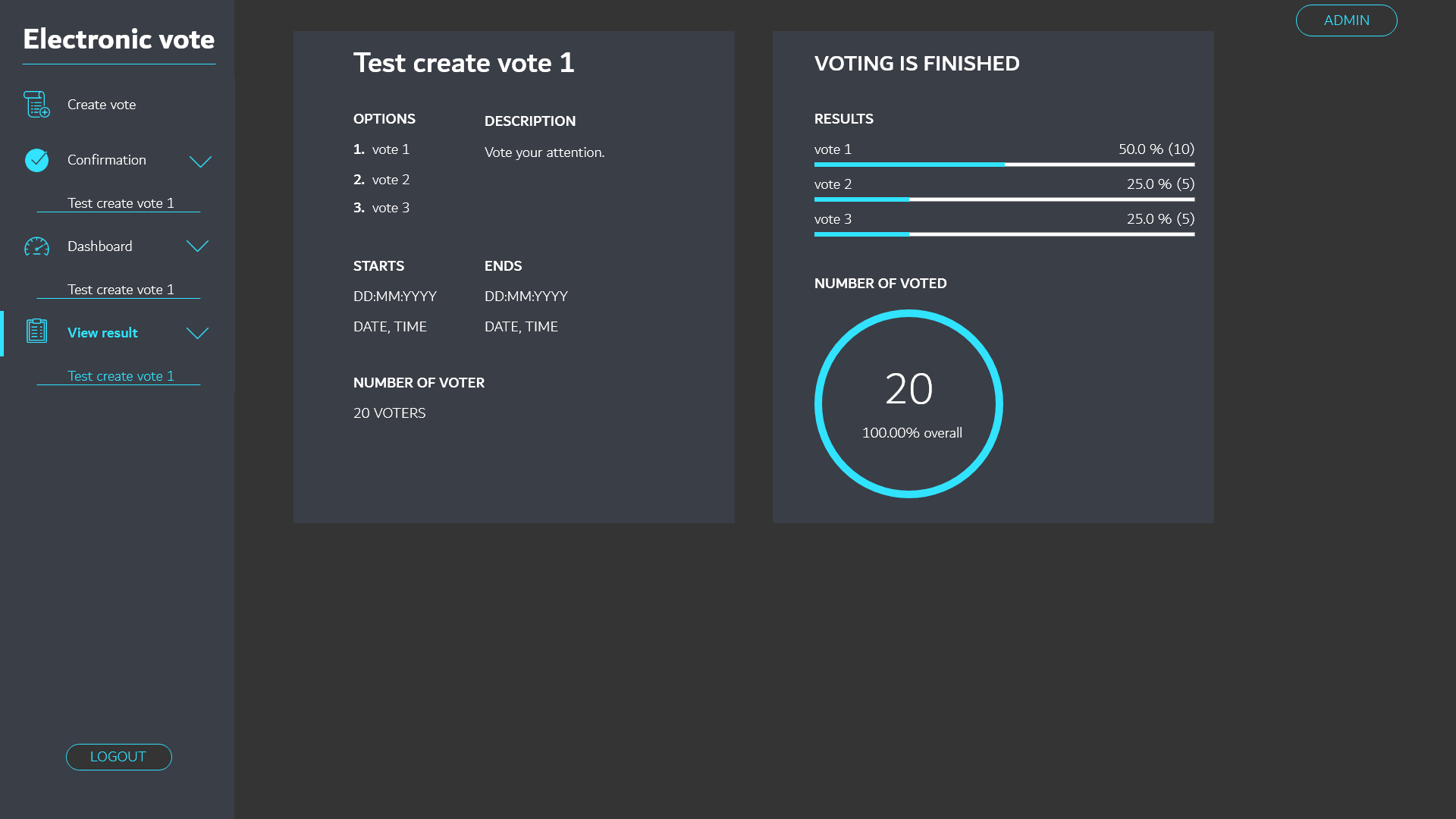
#### 4.1.6 หน้าข้อมูลการลงคะแนนเสียงและจำนวนผู้ที่ลงคะแนน

ในหน้านี้จะแสดงถึงข้อมูลการลงคะแนนที่ทางผู้จัดตั้งการลงคะแนนเสียงได้ทำการสร้างขึ้นมาเพื่อดูรายละเอียดและจำนวนคนที่ลงคะแนนไปแล้วในขณะนั้นดังรูปที่ 7



รูปที่ 4.7 หน้าแสดงข้อมูลการลงคะแนนเสียงและจำนวนผู้ที่ลงคะแนนเสียง

#### 4.1.7 หน้าแสดงผลคะแนนการโหวตทั้งหมด

แสดงข้อมูลผลสรุปจำนวนคะแนนทั้งหมดที่มีคนมาโหวตและจำนวนคนที่มาโหวตทั้งหมดดังรูปที่ 8

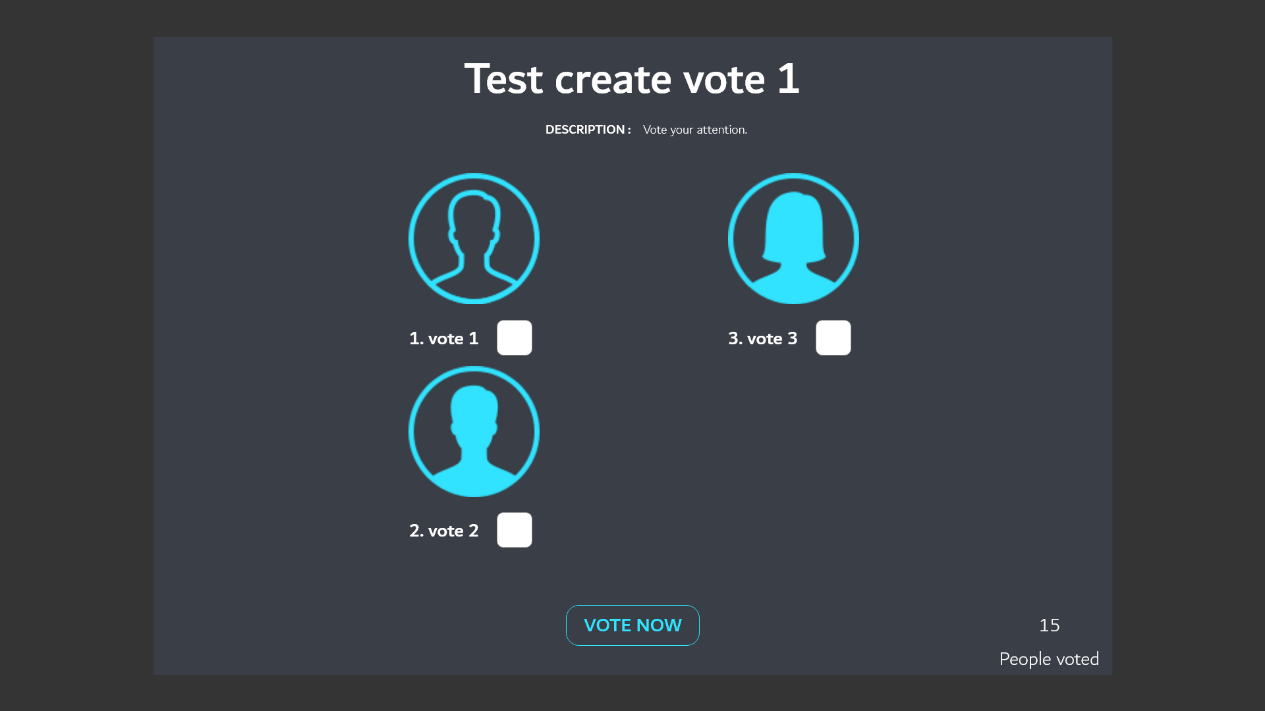
รูปที่ 4.8 หน้าแสดงผลคะแนนการโหวตทั้งหมด

## 

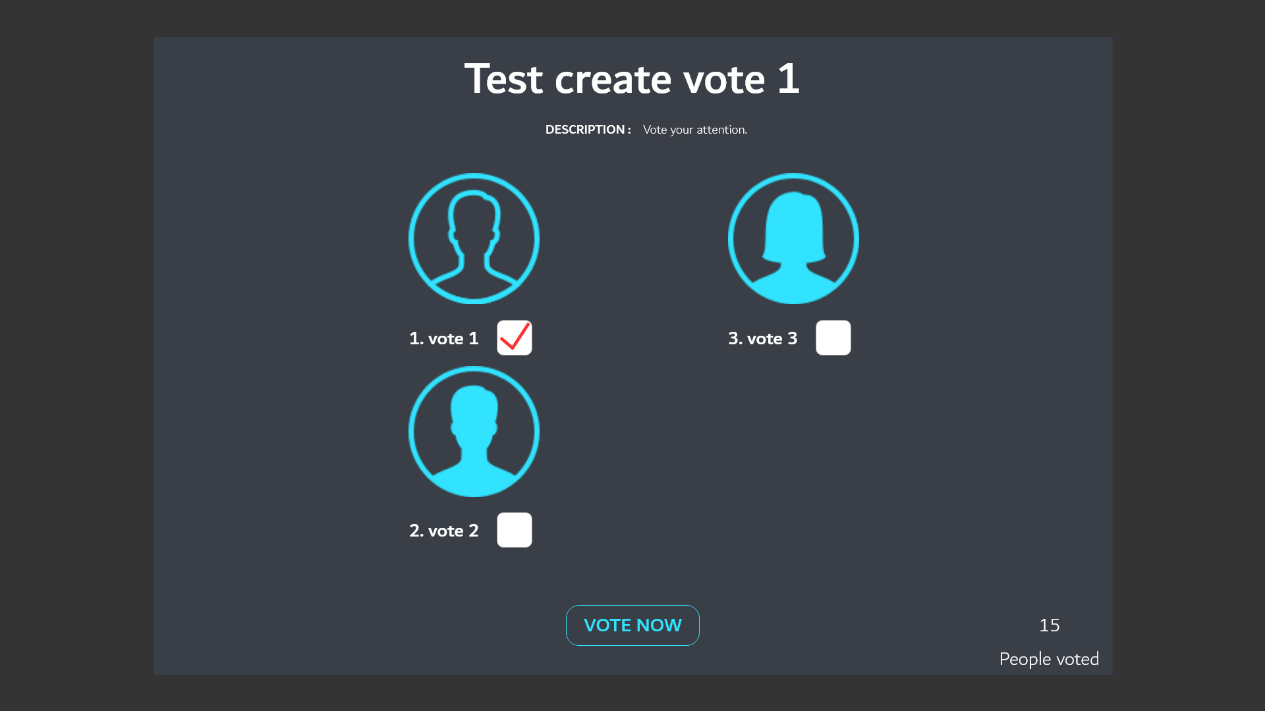
## 4.2 ส่วนที่ติดต่อกับผู้ลงคะแนนเสียง

เมื่อผู้ลงคะแนนทำการ Login โดยใช้เลขบัตรประจำตัวประชาชนและรหัสที่ได้รับมาจากผู้จัดตั้งการลงคะแนนเสียงจากรูปที่ 2 จะเข้าสู่หน้าลงคะแนนเสียงของผู้ลงคะแนน

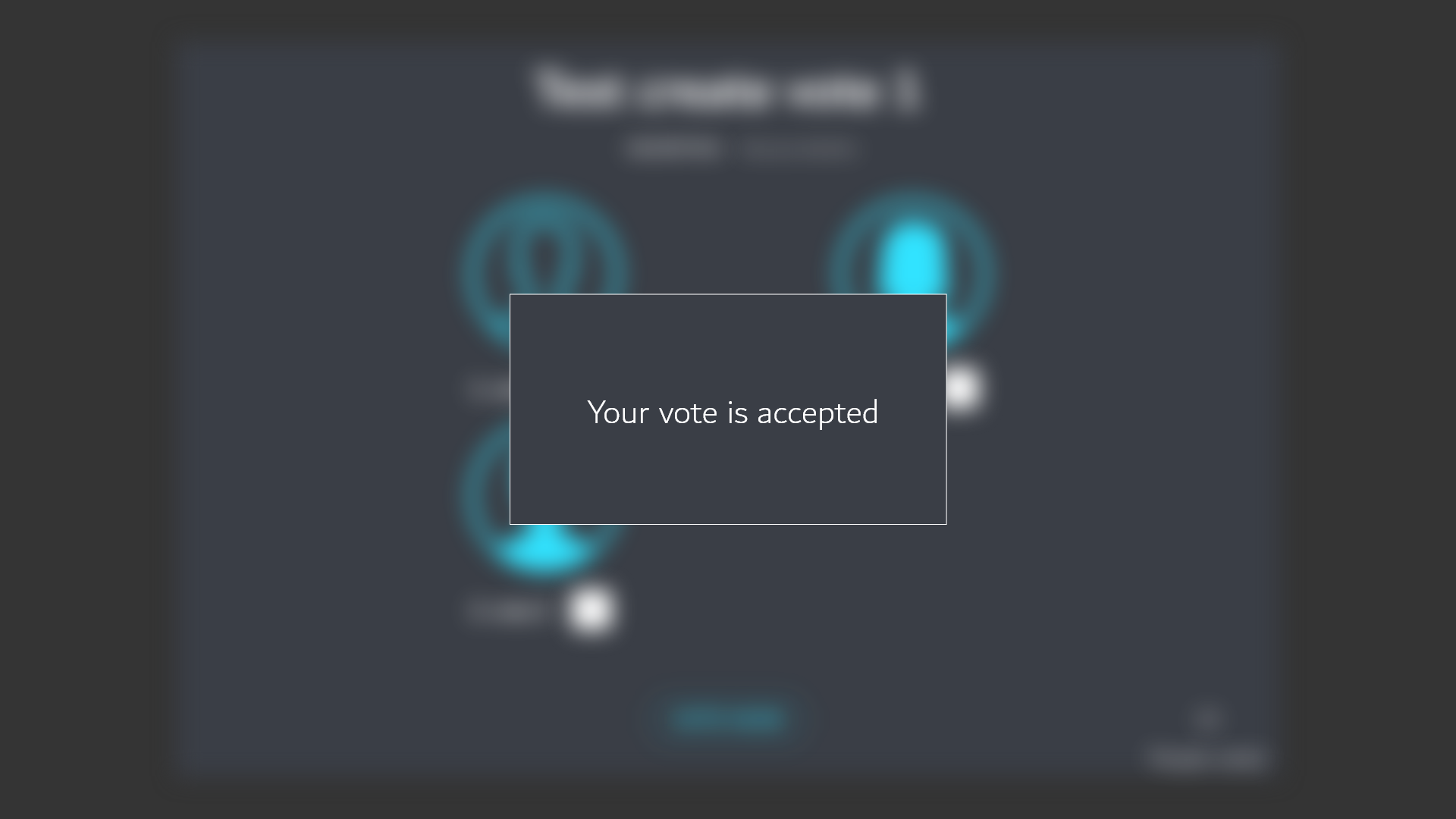
**4.2.1 หน้าลงคะแนนเสียงของผู้ลงคะแนน**

เมื่อผู้ลงคะแนนทำการ Login สำเร็จจะมายังหน้าใช้สิทธิ์โหวตของผู้ลงคะแนน ดังรูปที่ 9 หลังใช้สิทธิ์ลงคะแนนเสียงของตนเองดังรูปที่ 10-11 แสดงว่าการลงคะแนนสำเร็จ

รูปที่ 4.9 หน้าลงคะแนนเสียงของผู้ลงคะแนน

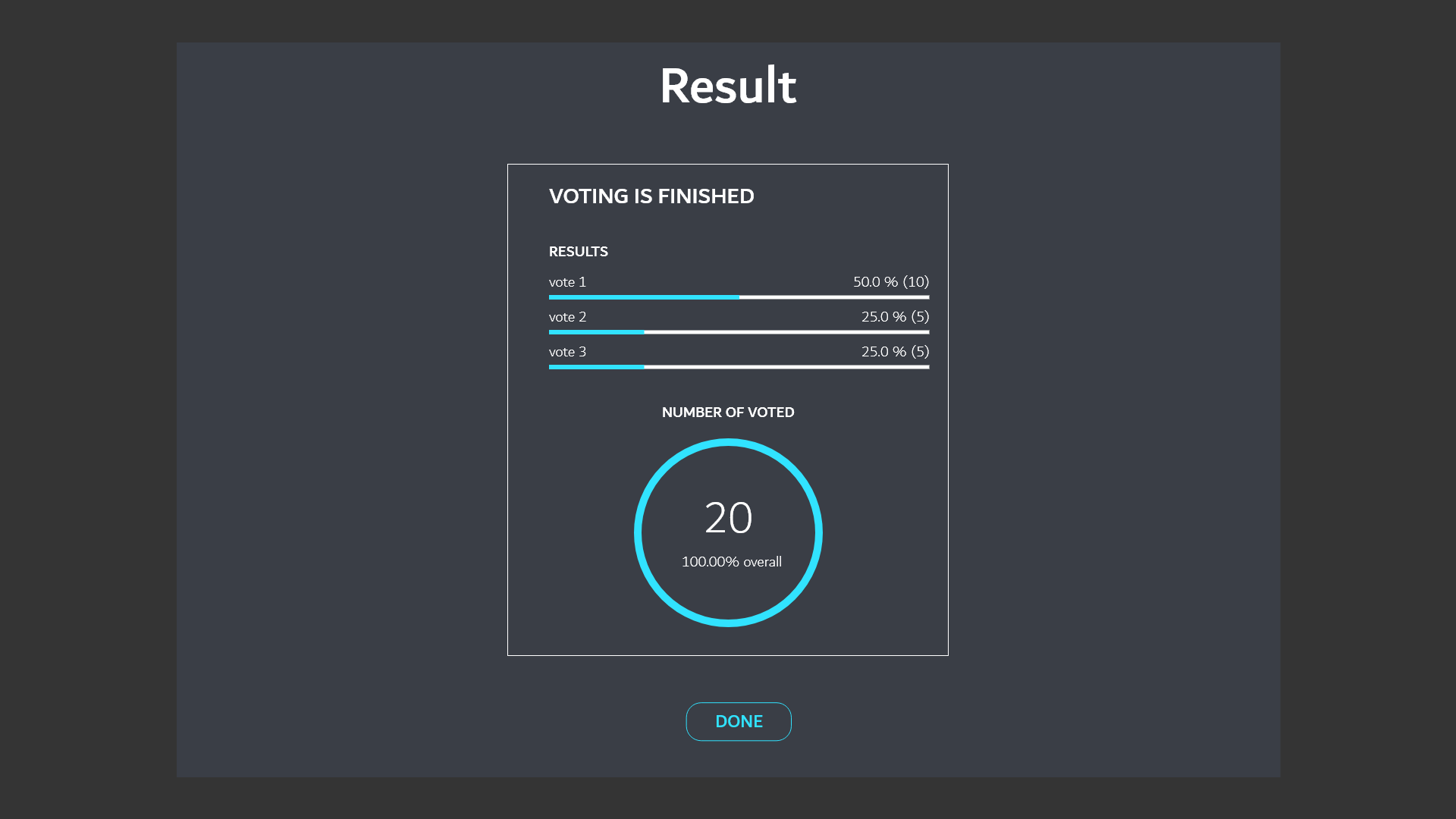


รูปที่ 4.10 ผู้ลงคะแนนใช้สิทธิ์ลงคะแนนเสียงของตนเอง



รูปที่ 4.11 การลงคะแนนเสียงสำเร็จ

#### 4.2.2 หน้าแสดงผลการลงคะแนนเสียงทั้งหมด

เมื่อผู้ลงคะแนนทำการ Login โดยใช้เลขบัตรประจำตัวประชาชนและรหัสหลังจากการลงคะแนนเสียงได้ปิดระบบแล้วจะเข้าสู่หน้าดูผลการลงคะแนนเสียงทั้งหมดดังรูปที่ 12

รูปที่ 4.12 หน้าแสดงผลการลงคะแนนเสียงทั้งหมด

## 4.3 ผลการทดลองเชื่อมต่อ Blockchain เบื้องต้น

วิธีการสร้าง Ethereum blockchain node นำมาใช้เชื่อมต่อกันเพื่อทำการ synchronize ข้อมูลภายใน blockchain ให้เหมือนกันโดยใช้คอมพิวเตอร์ จำนวน 2 เครื่องสร้างเป็น node [3]

การสร้าง Ethereum blockchain node จะแบ่งเป็น 2 ส่วนหลักๆคือ

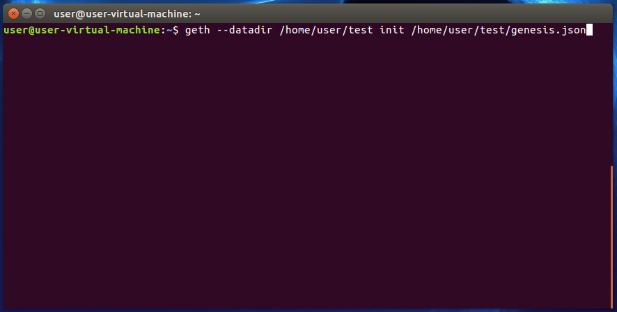
#### 4.3.1 การสร้าง Node

คอมพิวเตอร์เครื่องที่ 1

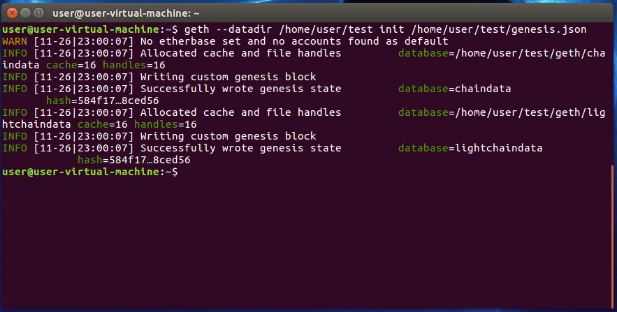
สร้างไฟล์ genesis.json เพื่อใช้สำหรับการ Initialization สำหรับคอมพิวเตอร์ทั้งสองเครื่องโดยที่ค่าพารามิเตอร์ภายในไฟล์ จะต้องมีค่าเหมือนกัน



รูปที่ 4.13 แสดงการเขียนพารามิเตอร์ในไฟล์ genesis.json



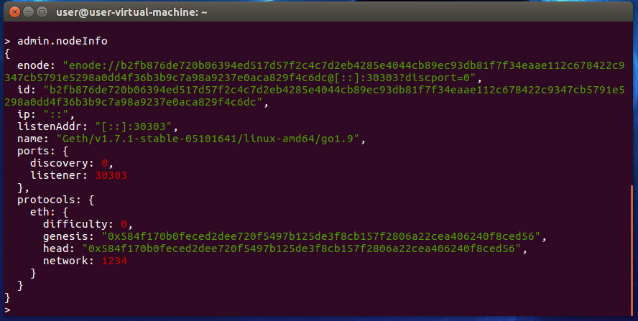
รูปที่ 4.14 แสดงคำสั่งการ Initialization ด้วยไฟล์ genesis.json ที่ได้สร้างขึ้น



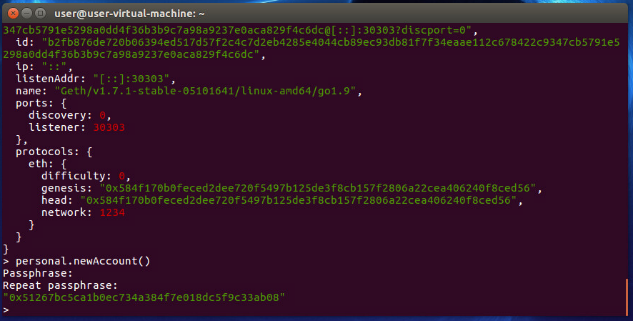
รูปที่ 4.15 แสดงผลลัพธ์จากการพิมคำสั่ง Initialization ไฟล์ genesis.json



รูปที่ 4.16 แสดงผลลัพธ์จากการพิมคำสั่งของ geth เพื่อเข้าสู่ console

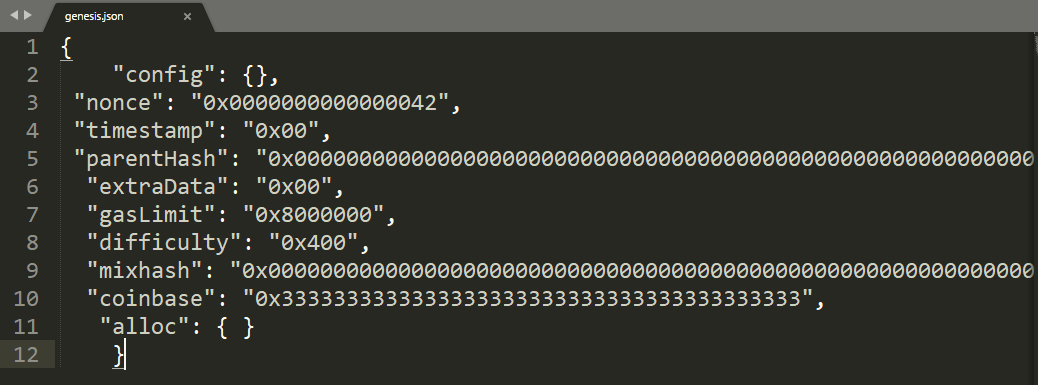


รูปที่ 4.17 แสดงผลลัพธ์จากการใช้คำสั่ง admin.nodeInfo

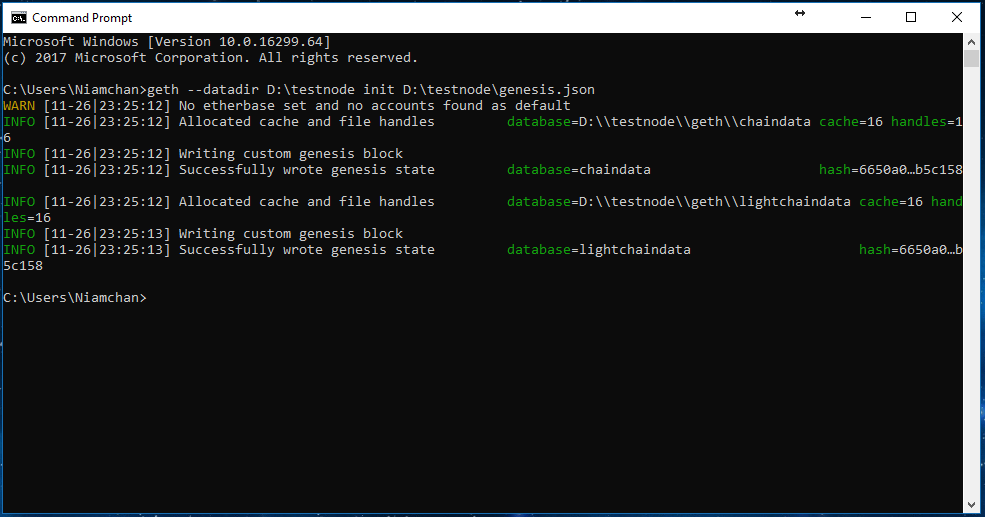


รูปที่ 4.18 แสดงผลลัพธ์จากการใช้คำสั่ง personal.newAccount()

คอมพิวเตอร์เครื่องที่ 2

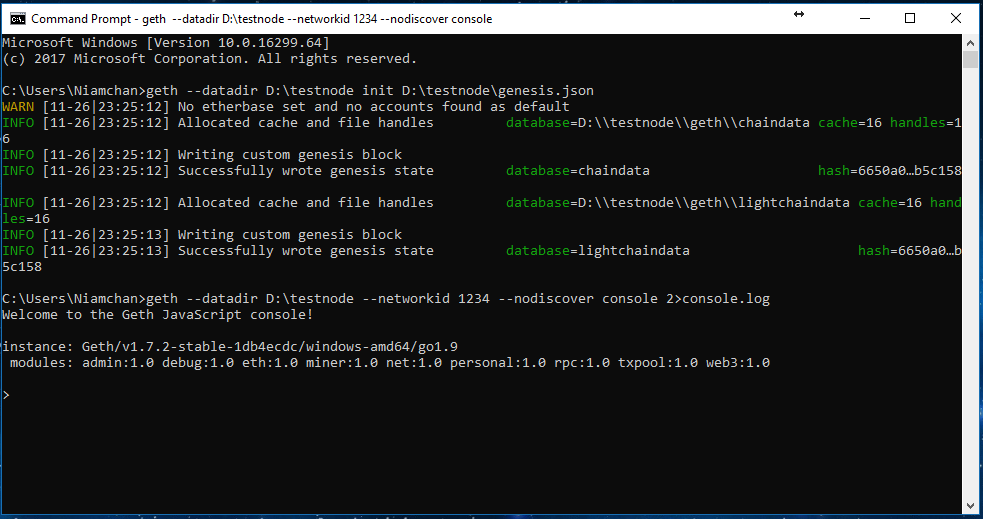


รูปที่ 4.19 แสดงการเขียนพารามิเตอร์ในไฟล์ genesis.json

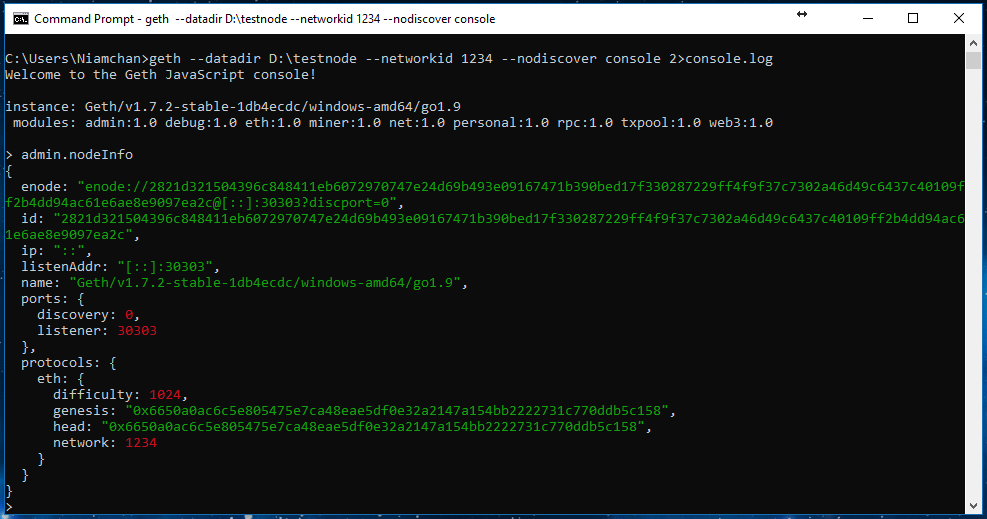


รูปที่ 4.20 แสดงคำสั่งการ Initialization ด้วยไฟล์ genesis.json

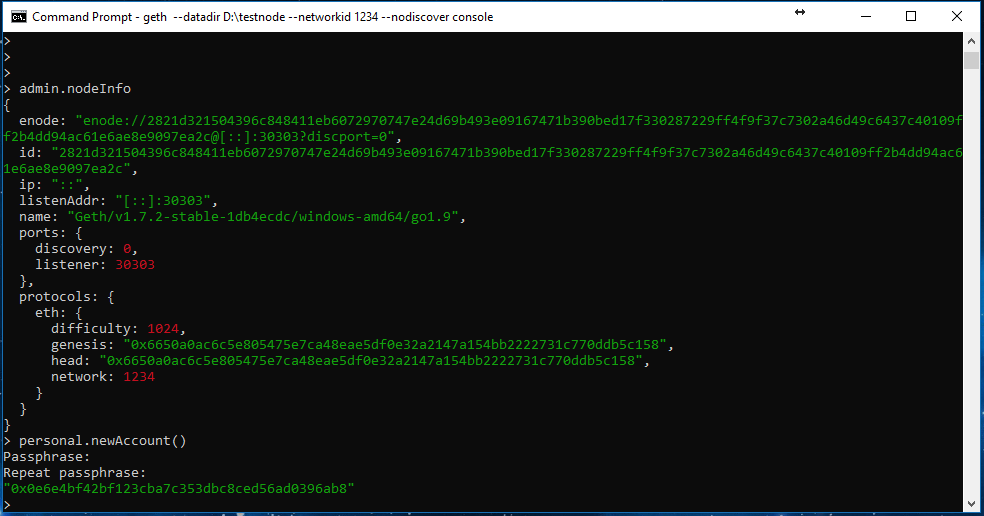
ที่ได้สร้างขึ้นและแสดงผลลัพธ์



รูปที่ 4.21 แสดงคำสั่งและแสดงผลลัพธ์ เพื่อเข้าสู่ console

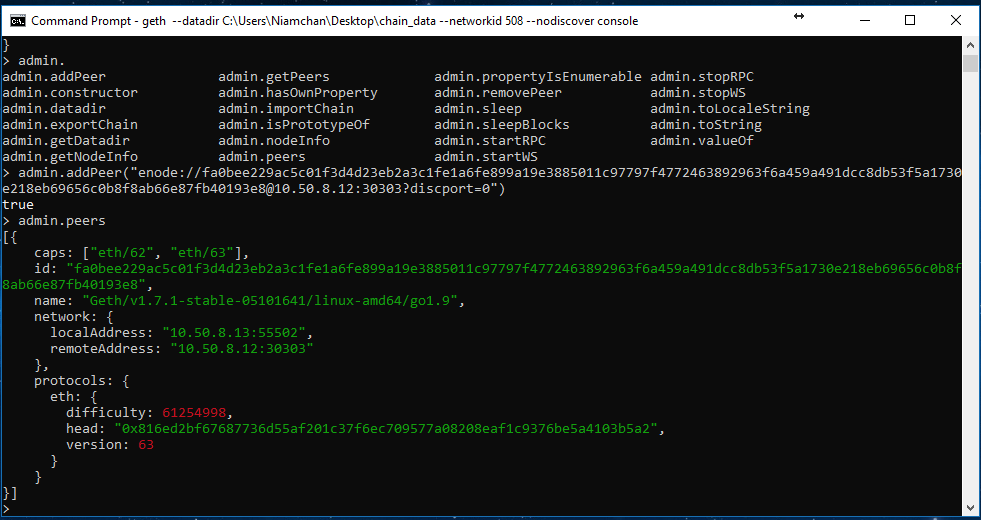


รูปที่ 4.22 แสดงผลลัพธ์จองการใช้คำสั่ง admin.nodeInfo



รูปที่ 4.23 แสดงผลลัพธ์จากการใช้คำสั่ง personal.newAccount()

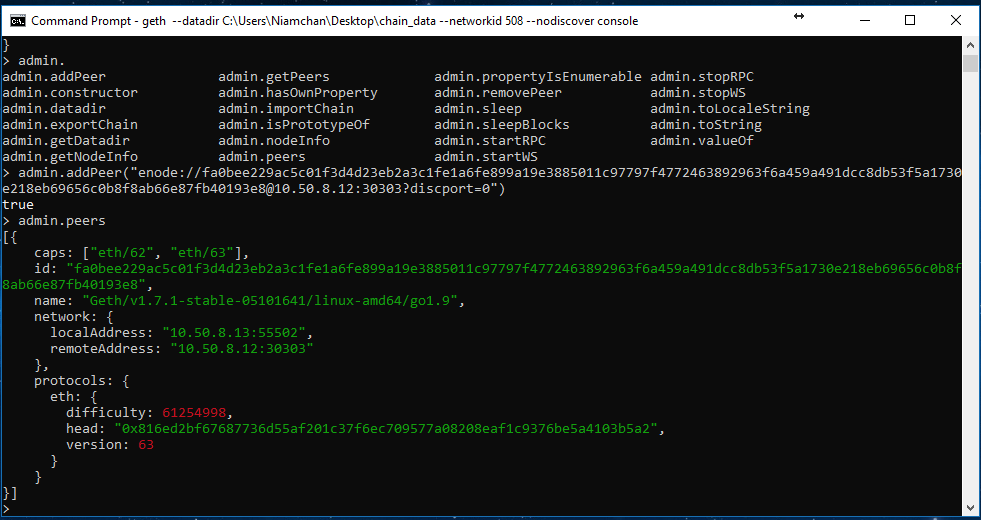
#### 4.3.2 การ Synchronize ข้อมูล



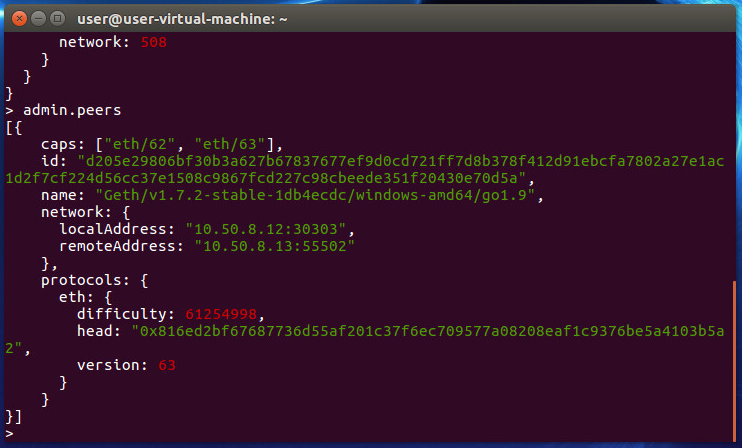
รูปที่ 4.24 แสดงการใช้คำสั่งเพื่อเชื่อมต่อระหว่างคอมพิวเตอร์

ด้วย enode ของ node จากคอมพิวเตอร์ตัวแรก

ใช้คำสั่ง admin.peers เพื่อทำการเรียกดูข้อมูลของ node ที่ทำการเชื่อมต่อเข้ามา

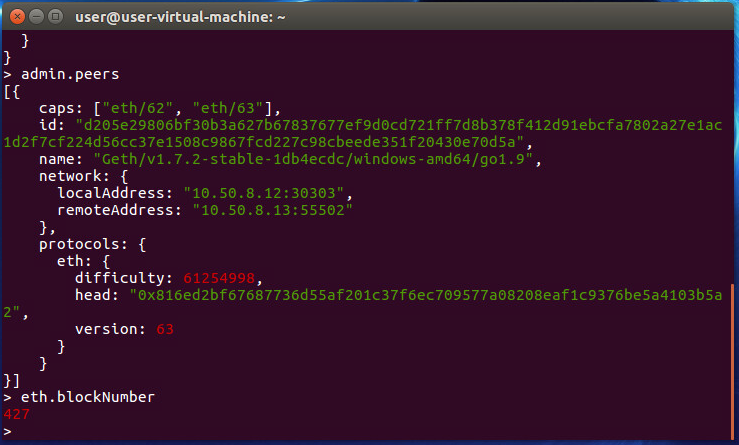


รูปที่ 4.25แสดงผลลัพธ์จากคอมพิวเตอร์เครื่องที่ 2 โดยใช้คำสั่ง admin.peers

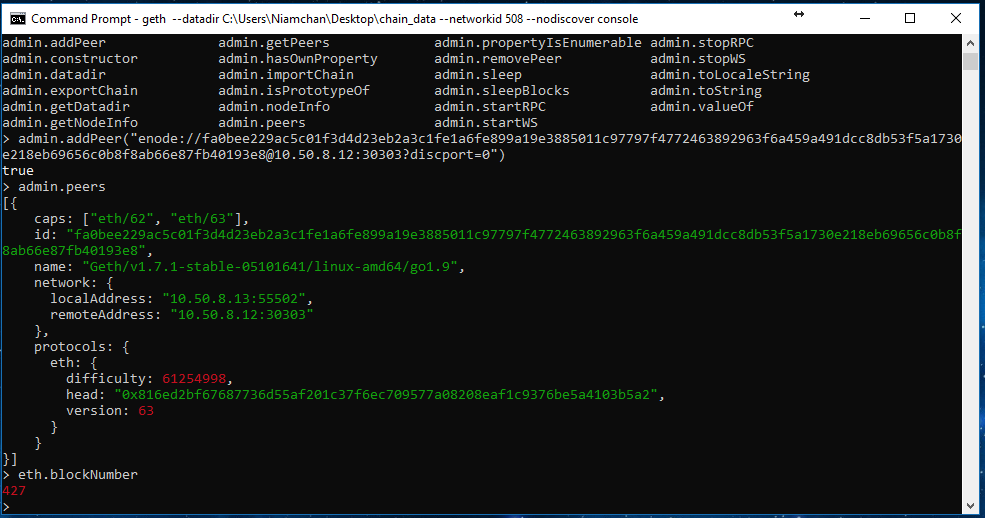


รูปที่ 4.26 แสดงผลลัพธ์จากคอมพิวเตอร์เครื่องที่ 1 โดยใช้คำสั่ง admin.peers

ใช้คำสั่ง eth.blockNumber เพื่อตรวจสอบจำนวน block ที่อยู่ในระบบของ node ที่ 1 ว่ามีจำนวนเท่าไหร่แล้วนำไปตรวจสอบกับ node ที่ 2 ว่ามีจำนวนเท่ากันหรือไม่โดยใช้คำสั่งเดียวกัน



รูปที่ 4.27 แสดงผลลัพธ์จากคอมพิวเตอร์เครื่องที่ 1 โดยใช้คำสั่ง eth.blockNumber



รูปที่ 4.28 แสดงผลลัพธ์จากคอมพิวเตอร์เครื่องที่ 2 โดยใช้คำสั่ง eth.blockNumber

# บทที่ 5

**สรุปผลดำเนินงาน**

## 5.1 สรุปผลการดำเนินงาน

โครงงานฉบับนี้ได้นำเสนอระบบลงคะแนนเสียงอิเล็กทรอนิกส์ ทำงานบนเว็บแอพพลิเคชั่น โดยมี blockchain เป็นเทคโนโลยีในการทำงานเบื้องหลัง และเครื่องมือที่ใช้ในการพัฒนาได้แก่ Html, JavaScript

การออกแบบและพัฒนาระบบจะเน้นไปทางด้านรักษาความปลอดภัยของข้อมูลเป็นหลักเนื่องจากระบบเดิมการรักษาความปลอดภัยของข้อมูลยังทำได้ไม่เต็มประสิทธิภาพ การลงคะแนนเสียงแบบเดิมเป็นการทำเครื่องหมายบนกระดาษแล้วนำไปใส่ในภาชนะที่ปิดสนิทโดยหน่วยงานจะเตรียมไว้แล้วถูกเคลื่อนย้ายไปรวมกันในจุดนับคะแนน ผู้ลงคะแนนไม่สามารถรู้ได้เลยว่าระหว่างที่ผลคะแนนถูกเคลื่อนย้าย จะมีการเปลี่ยนผลการลงคะแนนในที่เก็บผลลงคะแนนหรือไม่ ทำให้เกิดข้อสงสัยในด้านความปลอดภัยและความโปร่งใส่ในวิธีการลงคะแนนเสียงในปัจจุบัน

ระบบจึงได้รับการออกแบบใหม่ให้เพิ่มความปลอดภัยของข้อมูลมากขึ้นโดยใช้เทคโนโลยี Blockchain เป็นเทคโนโลยีสำหรับการเก็บข้อมูลแบบกระจาย ออกแบบมาเพื่อความปลอดภัยและความถูกต้องของข้อมูลโดยเฉพาะ โครงสร้างของการเก็บข้อมูลในเทคโนโลยีนี้ข้อมูลจะถูกเก็บเป็นชุดข้อมูลที่เรียกว่า “บล็อค” ซึ่งข้อมูลที่ถูกเก็บลงบล็อกแล้วจะไม่สามารถแก้ไขเปลี่ยนแปลงหรือลบได้ มีความเชื่อมโยงกันระหว่างบล็อคก่อนหน้าและบล็อคถัดไปอีกด้วย จึงทำให้ไม่สามารถลบออกได้เพราะจะทำให้ความต่อเนื่องของลำดับของบล็อคผิดไป และเมื่อนำมาใช้กับระบบลงคะแนนเสียงอิเล็กทรอนิกส์จึงทำให้เกิดความปลอดภัยต่อข้อมูลอย่างมาก โดยระบบจะทำงานเป็น 2 ส่วนได้แก่ ส่วนของผู้ลงคะแนนเสียง และส่วนของผู้จัดตั้งการลงคะแนนเสียง ในส่วนของผู้จัดตั้งการลงคะแนนเสียงจะสามารถจัดตั้งหัวข้อการลงคะแนนเสียงและกำหนดผู้เข้าร่วมลงคะแนนเสียง เมื่อจัดตั้งหัวข้อแล้วจะไม่สามารถแก้ไขอะไรได้แล้ว ในส่วนของผู้เข้าร่วมลงคะแนนก็จะสามารถเข้ามาลงคะแนนเสียงได้และสามารถดูผลสรุปการลงคะแนนเสียงได้หลังจากปิดการลงคะแนนแล้วเท่านั้น

## 5.2 ปัญหาและอุปสรรคที่พบ

1. ในการศึกษาหลักการทำงานของเทคโนโลยี blockchain ต้องใช้เวลาเนื่องจากเป็นเทคโนโลยีใหม่ทางทีมพัฒนาไม่มีความรู้ในเทคโนโลยีนี้เลยจึงต้องทำการศึกษาด้วยตัวเอง และข้อมูลของเทคโนโลยีนี้ส่วนใหญ่เป็นข้อมูลของต่างประเทศจึงต้องนำมาแปลเองและค่อยๆทำความเข้าใจ จึงใช้ระยะเวลาศึกษานานกว่าที่คาดการณ์ไว้ในการทำความเข้าใจหลักการทำงานและขอบเขตการทำงานของเทคโนโลยีนี้ได้

2. เนื่องจากผู้พัฒนาไม่มีความรู้ในการพัฒนาเว็บไซต์เบื้องหลัง ทำให้ต้องใช้เวลาศึกษาเพิ่มเติมเป็นเวลานานเกินกว่าที่คาดการณ์ไว้

## 5.3 ข้อจำกัดของระบบ

1. จำนวนของเครื่องตรวจสอบความถูกต้องยังมีอยู่น้อย จึงทำให้ขาดความน่าเชื่อถือในการตรวจสอบความถูกต้องของข้อมูลการลงคะแนน

# บรรณานุกรม

|  |  |
| --- | --- |
| [1] | S. Phanvilai., “Blockchain คืออะไร? อธิบายแบบละเอียด แต่เข้าใจง่าย(มั้ง),” [ออนไลน์]. Available: https://nuuneoi.com/blog/blog.php?read\_id=900. |
| [2] | J. Narktong, “Proof of Work vs Proof of Stake สิ่งที่นักขุดควรจะรู้ก่อนเริ่มขุด,” [ออนไลน์]. Available: https://siamblockchain.com/2017/08/13/proof-of-work-vs-proof-of-stake/. |
| [3] | H. jameson, “Creating a Private Chain/Testnet,” [ออนไลน์]. Available: https://souptacular.gitbooks.io/ethereum-tutorials-and-tips-by-hudson/content/private-chain.html. |

# บรรณานุกรม

[1] [Sittiphol Phanvilai](https://www.facebook.com/nuuneoi?hc_ref=ARS8WykQ1EKz6vg_PEYcd1c6HAN39dwnXocbSTh_0hEhOzKA1vDdXrH0Nfc5QcL5S7s&fref=nf). **“Blockchain คืออะไร? อธิบายแบบละเอียด แต่เข้าใจง่าย(มั้ง)”** [Online].

Available : <https://nuuneoi.com/blog/blog.php?read_id=900>

[2] Jiraboon Narktong **“Proof of Work vs Proof of Stake สิ่งที่นักขุดควรจะรู้ก่อนเริ่มขุด”** [Online]. Available : <https://siamblockchain.com/2017/08/13/proof-of-work-vs-proof-of-stake/>

[3] Hudson jameson. **“Creating a Private Chain/Testnet.”** [Online].

Available: [https://souptacular.gitbooks.io/ethereum-tutorials-and-tips-by-hudson/content/private-chain.html .2016](https://souptacular.gitbooks.io/ethereum-tutorials-and-tips-by-hudson/content/private-chain.html%20.2016)

[4] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, J. Alex Halderman **“Security Analysis of the Estonian Internet Voting System”** [Online]. Available : <https://jhalderm.com/pub/papers/ivoting-ccs14.pdf>

[5] Andrew Barnes, Christopher Brake and Thomas Perry. **“Digital Voting with the use of Blockchain Technology”**

[6] Jim Krurose and Keith Ross. Computer Networking : A Top-Down Approach 6th edition. Chapter 8 : Security.