การพัฒนาระบบเงินสดดิจิตอลชนิดออฟไลน์

DEVELOPMENT OF OFF-LINE DIGITAL CASH SYSTEM

โดย

ชนาธิป อิ่มทองคำ

CHANATIP IMTHONGKAM

อาจารย์ที่ปรึกษา

ดร. นล เปรมัษเฐียร

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 2 ปีการศึกษา 2554

DEVELOPMENT OF OFF-LINE DIGITAL CASH SYSTEM

CHANATIP IMTHONGKAM

A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS OF THE COURSE

INDEPENDENT STUDY 2

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2/2011

หัวข้อ	การพัฒนาระบบเงินสดดิจิตอลชนิดออฟไลน์
นักศึกษา	นายชนาธิป อิ่มทองคำ
รหัสนักศึกษา	52660549
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีระบบสารสนเทศ
ปีการศึกษา	2554
อาจารย์ที่ปรึกษา	ดร.นล เปรมัษเฐียร

บทคัดย่อ

ปริญญานิพนธ์ฉบับนี้ นำเสนอระบบเงินสดดิจิตอลดิจิตอลชนิดออฟไลน์ ซึ่งเป็นระบบเงินสดที่สามารถให้ความเป็นส่วนตัวกับผู้ใช้ เช่นเดียวกับเงินสด และมีความปลอดภัยจากการที่ไม่ต้องถือเงินสดเป็นจำนวนมากติดตัว เช่นเดียวกับเงินสดดิจิตอล จากการทำงานร่วมกันของระบบย่อย 3 ระบบ ได้แก่ ระบบแลกเปลี่ยนเงินสดดิจิตอล ระบบเงินสดดิจิตอลสำหรับร้านค้า และระบบเงินสดดิจิตอลสำหรับผู้ดูแลระบบ โดยการนำทฤษฎี และวิทยาการที่เกี่ยวกับการเข้ารหัสมาเป็นพื้นฐานในการพัฒนาระบบนี้ขึ้น ซึ่งระบบเงินสดดิจิตอลชนิดออฟไลน์นี้พัฒนาขึ้นเพื่อเพิ่มตัวเลือกทางเลือกการพาณิชย์อิเล็กทรอนิกส์ที่มีความต้องการหลายมากขึ้นในปัจจุบัน

Title	Development of Off-Line Digital Cash
Student	Mr. Chanatip Imthongkam
Student ID	52660549
Degree	Master of Science
Program	Information Technology
Major	Information System Technology
Year	2011
Advisor	Dr. Nol Premasathian

ABSTRACT

The Thesis proposes "Off-line Digital Cash Systems", that provides privacy of using cash and safety by not carry lot of money similar to credit card usage. It consists of 3 subsystems, including Digital Cash Exchange System, Digital Cash Shop System and Digital Cash Administrator System. Theory and methods of cryptography are the main foundation for development. This system developed to make more choices for electronics payment nowadays.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้ไม่อาจบรรลุผลสำเร็จได้ หากขาดความกรุณาจากอาจารย์ที่ปรึกษา ดร.นล เปรมัษเฐียร ที่ให้ความกรุณา ความช่วยเหลือ คำแนะนำที่ดี ในการพัฒนาโครงการและการปรับปรุง แก้ไขปัญหาต่างๆ มาโดยตลอด

ขอขอบคุณพ่อ แม่ ป้า น้า ยาย และน้องมิ้นท์ ที่คอยสนับสนุน และช่วยเหลือมาโดยตลอด

ขอขอบคุณอาจารย์ทุกท่านที่ได้ให้ความรู้ที่มีประโยชน์ ช่วยให้สามารถแก้ไขปัญหาต่างๆ ให้สำเร็จลุล่วงไปได้ และเป็นตัวอย่างที่ดีในการศึกษาเล่าเรียนและการทำงาน

ขอขอบคุณคณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังที่เอื้ออำนวยสภาพแวดล้อมต่างๆ ในการทำโครงงาน

สุดท้ายนี้ขอขอบคุณเพื่อนๆ พี่น้อง และเจ้าหน้าที่ฝ่ายทะเบียนคณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกคนที่ได้ให้การช่วยเหลือและกำลังใจ เพื่อให้โครงงานชิ้นนี้สำเร็จลุล่วงได้โดยสมบูรณ์

ชนาธิป อิ่มทองคำ

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญรูป

สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ด้วยความก้าวหน้าของเทคโนโลยี ส่งผลให้รูปแบบการใช้ชีวิตของคนในปัจจุบันรวมทั้งปัจจัยที่จำเป็นต่อการใช้ชีวิตเปลี่ยนไป หลายสิ่งหลายอย่างเกี่ยวข้องกับเทคโนโลยี และอิเล็กทรอนิกส์ไปเสียหมด ซึ่งความเจริญเหล่านี้ช่วยให้การดำเนินชีวิตสะดวก และง่ายขึ้น แต่ในขณะเดียวกันอาจเป็นสาเหตุหนึ่งที่ทำให้ปลอดภัยของการใช้ชีวิต และทรัพย์สินอยู่บนความเสี่ยงได้เช่นเดียวกัน

หากย้อนไปประมาณ 20-30 ปีก่อน คนในสมัยนั้นใช้เงินสดในการจับจ่ายสินค้าเพียงอย่างเดียว แต่เมื่อเทคโนโลยีมีการพัฒนาก้าวหน้ามากขึ้น ทำให้การดำเนินชีวิตเปลี่ยนไป รูปแบบการซื้อขายสินค้ามีให้เลือกหลากหลายมากขึ้น ซึ่งภายในระบบเหล่านั้น ซ่อนไว้ซึ่งการทำงานที่ซับซ้อน ทำให้เกิดการคิดค้นการชำระค่าสินค้ารูปแบบใหม่ๆ เพื่อเป็นทางเลือกในการอำนวยความสะดวกให้ลูกค้ากับผู้ดำเนินธุรกิจ ดังเช่นรูปแบบการชำระเงินที่ได้รับความนิยมในปัจจุบัน อาทิ ธนบัตร บัตรเอทีเอ็ม เช็ค บัตรเครดิต รวมทั้งระบบการชำระเงินอิเล็กทรอนิกส์อื่นๆ ซึ่งการชำระเงินเหล่านี้มีข้อดี และข้อเสียแตกต่างกันไป แต่สิ่งหนึ่งที่หลีกเลี่ยงไม่ได้หากเลือกใช้บริการของบัตรเงินสดหรือบัตรเครดิต คือ การชำระเงินผ่านระบบอิเล็กทรอนิกส์เหล่านี้ ต้องมีชื่อลูกค้าแนบไปกับรายการชำระเงินทุกครั้ง ลูกค้าไม่สามารถปิดบังรายการการซื้อสินค้าจากร้านค้าได้ แตกต่างจากการใช้จ่ายโดยเงินสด ทำให้เกิดปัญหาบางประการตามมา เช่น การละเมิดสิทธิส่วนบุคคลของผู้บริโภค เนื่องจากมีกลไกที่สามารถค้นหาข้อมูลพฤติกรรมการซื้อของผู้บริโภค ซึ่งมีความเป็นไปได้ที่บุคคลบางกลุ่มที่มีความสนใจในการค้นหาข้อมูลส่วนบุคคลทราบถึงรายละเอียดข้อมูลได้

จากข้อจำกัดของบัตรเครดิต และบัตรเอทีเอ็มที่สามารถทราบถึงข้อมูลผู้ใช้ และร้านค้าที่ใช้บริการนั้นได้ รวมถึงระบบเอทีเอ็ม และบัตรเครดิตนี้ยังต้องอาศัยการทำงานแบบออนไลน์ คือ ร้านค้าที่รองรับการให้บริการต้องสามารถติดต่อกับธนาคารได้ตลอดเวลา ทำให้ค่าใช้จ่ายของระบบสูง แตกต่างจากระบบเงินสด ประกอบกับการที่สามารถรักษาความเป็นส่วนตัวได้ อีกทั้งยังไม่จำเป็นที่ระบบต้องติดต่อกับธนาคารตลอดเวลา ทางคณะผู้จัดทำจึงเกิดแนวคิดที่จะพัฒนาระบบชำระเงินที่ให้ความสำคัญกับการรักษาความลับของข้อมูลส่วนตัวของผู้ใช้เป็นหลักที่สามารถตรวจสอบผู้กระทำผิดได้ หากเกิดเหตุการณ์ทุจริต โดยการนำข้อดีของบัตรเครดิต และบัตรเอทีเอ็มที่ให้ความปลอดภัยกับผู้ใช้ โดยการที่ไม่ต้องถือเงินสดจำนวนมาก ผสมผสานกับคุณสมบัติของเงินสดที่สามารถรักษาความลับของผู้ใช้ได้ จึงเกิดเป็นแนวคิดการพัฒนาระบบเงินสดดิจิตอลชนิดออฟไลน์ขึ้น

1.2 วัตถุประสงค์

1.2.1 เพื่อศึกษาหลักการ และทฤษฎีวิทยาการการเข้ารหัส (Cryptography)

1.2.2 ออกแบบระบบเงินสดดิจิตอลแบบออฟไลน์ที่สามารถรักษาความเป็นส่วนตัวของผู้ใช้ได้ เช่น เดียวกับคุณสมบัติของเงินสด

1.2.3 พัฒนาระบบเงินสดดิจิตอลชนิดออฟไลน์ คือ ระบบของร้านค้าไม่ต้องเชื่อมต่อกับธนาคารขณะซื้อขายสินค้า

1.3 สมมติฐานของการศึกษา

ระบบเงินสดดิจิตอลชนิดออฟไลน์ที่พัฒนาขึ้นเป็นระบบที่สามารถสร้างเงินสดดิจิตอล และสามารถใช้เงินสดดิจิตอลชำระค่าสินค้า หรือบริการกับร้านค้าที่มีซอฟต์แวร์ของระบบดิจิตอลสำหรับร้านค้าติดตั้งอยู่ โดยระบบสามารถรักษาความลับข้อมูลผู้ใช้ได้เช่นเดียวกับเงินสด คือ ไม่สามารถตรวจสอบหาเจ้าของเงิน หรือผู้ใช้เงินได้ แต่ระบบสามารถตรวจสอบผู้ใช้เงินได้หากมีการทุจริต หรือการใช้เงินซ้ำเกิดขึ้น โดยกำหนดให้ผู้กระทำการทุจริตมีโทษทางกฎหมาย

1.4 วิธีการดำเนินการโครงงาน

1.4.1 ศึกษาวิทยาการเข้ารหัสลับ (Cryptography)

1.4.2 ศึกษาระบบเงินสดดิจิตอลแบบต่างๆ

1.4.3 ศึกษาขั้นตอน และโพรโตคอลของวิทยาการเข้ารหัสลับที่ใช้ในระบบเงินสดดิจิตอลชนิดออฟไลน์ ที่สามารถรักษาความเป็นส่วนตัวของผู้ใช้ได้

1.4.4 ออกแบบระบบเงินสดดิจิตอลชนิดออฟไลน์ที่ประยุกต์หลักการ และทฤษฎีของวิทยาการเข้ารหัสลับ เพื่อให้ระบบสามารถรักษาความเป็นส่วนตัวของผู้ใช้ได้

1.4.5 พัฒนาระบบเงินสดดิจิตอลชนิดออฟไลน์ตามที่ออกแบบไว้

1.4.6 ทดสอบการใช้งานของระบบเงินสดดิจิตอลชนิดออฟไลน์ที่พัฒนาขึ้น

1.4.7 สรุปผล และข้อเสนอแนะสำหรับพัฒนาระบบเพิ่มเติมในอนาคต

1.5 ขอบเขตของโครงการ

1.5.1 ลักษณะของระบบที่จะพัฒนา

1.5.1.1 ทำงานบนซอฟต์แวร์โดยไม่ต้องการฮาร์ดแวร์เฉพาะ

1.5.1.2 ระบบสามารถสร้างเงินสดดิจิตอลได้จากเงินสดที่มีอยู่ในบัญชีของผู้ใช้

1.5.1.3 ระบบสามารถคืนเงิน หรือขึ้นเงินสดดิจิตอลใช้แล้วให้เป็นเงินสดได้

1.5.1.4 ระบบของร้านค้าไม่ต้องติดต่อกับธนาคารขณะมีการซื้อขายสินค้า

1.5.1.5 ระบบสามารถตรวจสอบผู้ทุจริตได้หากมีการใช้เงินสดดิจิตอลซ้ำ

1.5.1.6 ระบบเงินสดดิจิตอลนี้ไม่มีเทคนิคการถ่ายโอนเงินอิเล็กทรอนิกส์ รวมทั้งเทคนิคการแตกเงินอิเล็กทรอนิกส์

1.5.1.7 ระบบให้ความเป็นส่วนตัวกับผู้ใช้ โดยจะไม่สามารถระบุตัวตนผู้ใช้เงินได้ หากไม่เกิดการทุจริต

1.5.2 องค์ประกอบของระบบเงินสดดิจิตอลชนิดออฟไลน์ ประกอบด้วย 3 ระบบย่อย

1.5.2.1 ระบบแลกเปลี่ยนเงินสดดิจิตอล

1.5.2.2 ระบบเงินสดดิจิตอลสำหรับร้านค้า

1.5.2.3 ระบบเงินสดดิจิตอลสำหรับผู้ดูแลระบบ

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 มีความรู้ความเข้าใจหลักการ และทฤษฎีเกี่ยวกับวิทยาการการเข้ารหัสเพิ่มมากขึ้น

1.6.2 พัฒนาทักษะการประยุกต์ความรู้ทางด้านเทคโนโลยีสารสนเทศ โดยเฉพาะวิทยาการการเข้ารหัส และนำทักษะดังกล่าวมาใช้กับระบบเงินสดดิจิตอลชนิดออฟไลน์ได้อย่างเหมาะสม

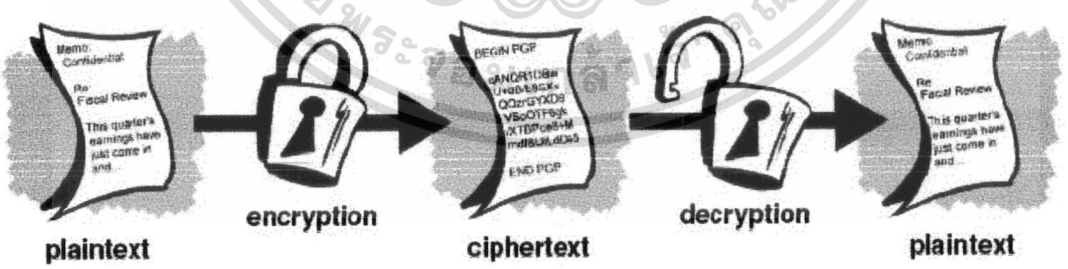
1.6.3 เป็นระบบต้นแบบอีกทางเลือกหนึ่งของการพาณิชย์อิเล็กทรอนิกส์ที่สามารถให้ความเป็นส่วนตัวกับผู้ใช้ได้

บทที่ 2
ทฤษฎีที่เกี่ยวข้องกับวิทยาการเข้ารหัสข้อมูล และระบบเงินสดดิจิตอล

เนื้อหาบทนี้กล่าวถึงภาพรวมทฤษฎีของวิทยาการการเข้ารหัสลับ และทฤษฎีที่เกี่ยวข้องกับระบบเงินสดดิจิตอล เพื่ออธิบายพื้นฐาน และหลักการของการพัฒนาระบบเงินสดดิจิตอลชนิดออฟไลน์

2.1 วิทยาการเข้ารหัสลับ (Cryptography)

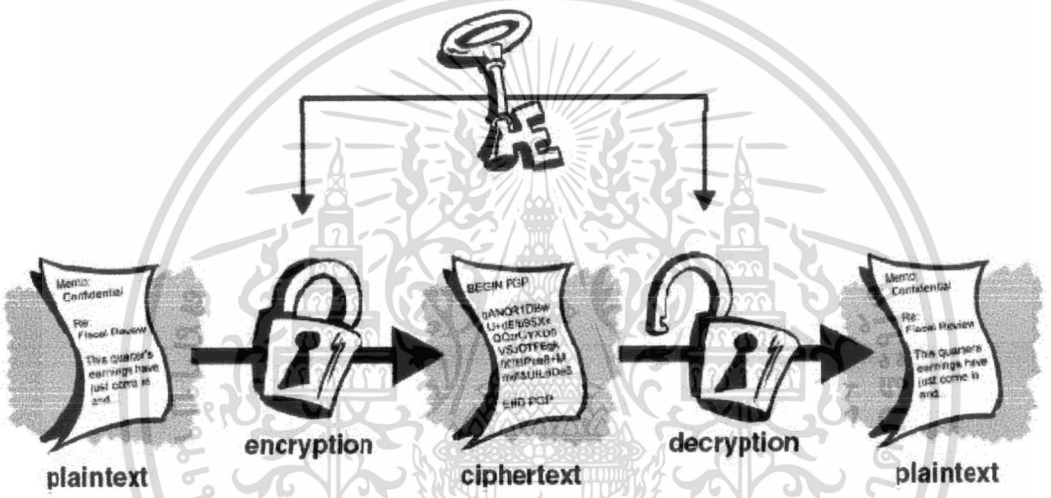
การเข้ารหัสข้อมูลโดยพื้นฐานแล้วเกี่ยวข้องกับวิธีการทางคณิตศาสตร์เพื่อใช้ในการป้องกันข้อมูลหรือข้อมูลตั้งต้นที่ต้องการส่งไปถึงผู้รับ ข้อมูลตั้งต้นที่สามารถอ่านได้ตามปกติ (Plaintext) จะถูกเปลี่ยนแปลงไปสู่ข้อมูล หรือข้อความอีกรูปแบบหนึ่งที่ไม่สามารถอ่านเข้าใจได้ (Ciphertext) โดยบุคคลทั่วไปที่ไม่มีกุญแจสำหรับเปิดดูข้อมูลนั้น เรียกกระบวนการในการแปลงข้อมูลตั้งต้นว่า "การเข้ารหัสข้อมูล" (Encryption) และกระบวนการในการแปลงข้อความที่ไม่สามารถอ่าน และทำความเข้าใจให้กลับไปสู่ข้อความดั้งเดิมว่า "การถอดรหัสข้อมูล" (Decryption) (บรรจง หะรังสี. 2547) จากรูปที่ 2.1 แสดงภาพการเข้ารหัส และถอดรหัสของข้อมูลโดยการเข้ารหัสสามารถแบ่งได้เป็น 2 รูปแบบ คือ การเข้ารหัสแบบสมมาตร (Symmetric Key Encryption) และการเข้ารหัสแบบอสมมาตร (Asymmetric Key Encryption)



รูปที่ 2.1 แสดงวิธีการเข้ารหัส (Anonymous. 2012)

2.1.1 การเข้ารหัสแบบสมมาตร (Symmetric Key Encryption)

อัลกอริทึมแบบนี้จะใช้กุญแจที่เรียกว่า กุญแจลับ (Secret key) ซึ่งมีเพียงหนึ่งเดียวเพื่อใช้ในการเข้าและถอดรหัสข้อความที่ส่งไปสามารถแบ่งย่อยอัลกอริทึมออกเป็น 2 ประเภท ได้แก่ แบบบล็อค (Block Algorithms) จะทำการเข้ารหัสทีละบล็อค (1 บล็อคประกอบด้วยหลายไบต์ เช่น 64 ไบต์ เป็นต้น) และแบบสตรีม (Stream Algorithms) ซึ่งจะทำการเข้ารหัสทีละไบต์ อัลกอริทึมแบบนี้จะใช้กุญแจที่เรียกว่า กุญแจลับ (Secret key) ที่มีเพียงตัวเดียวใช้ในการเข้าและถอดรหัสข้อความที่ส่งไป (บรรจง หะรังสี. 2547) ดังแสดงไว้ในรูปที่ 2.2

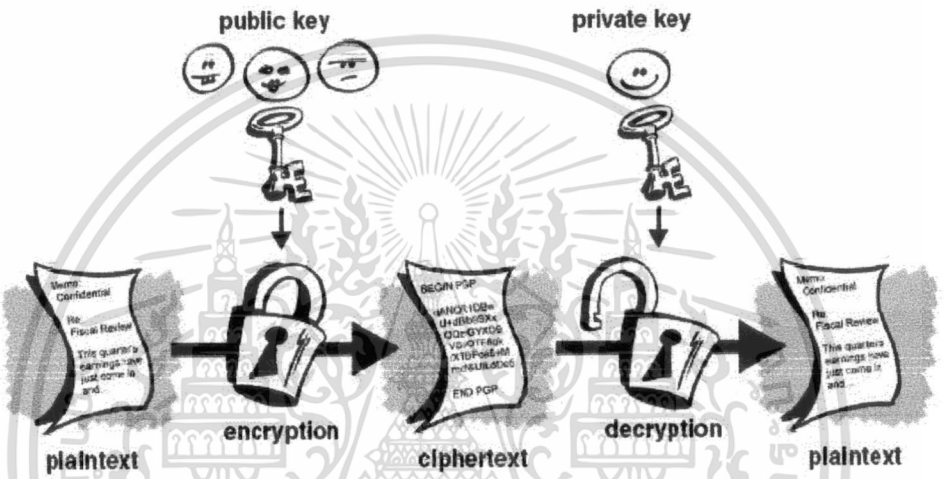


รูปที่ 2.2 การเข้ารหัสแบบสมมาตร (Anonymous. 2012)

การเข้ารหัสแบบสมมาตรมีข้อดี คือ ความสามารถในการทำงานที่รวดเร็ว เนื่องจากมีรูปแบบการทำงานที่ง่าย ทำให้การประมวลผลเพื่อเข้า และถอดรหัสทำได้อย่างรวดเร็ว นำมาซึ่งข้อจำกัด คือ การรักษาความลับของกุญแจทำได้ยาก เนื่องจากกุญแจเป็นส่วนสำคัญอย่างยิ่งของการเข้ารหัสแบบนี้ หากผู้อื่นสามารถขโมย หรือได้มาซึ่งกุญแจ จะทำให้การส่งข้อมูลไม่เป็นความลับอีกต่อไป โดยเฉพาะอย่างยิ่งหากเป็นการติดต่อสื่อสารข้ามเครือข่าย ทำให้โอกาสถูกลักลอบกุญแจเป็นไปได้สูงมากตามไปด้วย อีกทั้งในกรณีที่ผู้ส่งข้อมูล ต้องติดต่อสื่อสารกับผู้รับหลายกลุ่ม จากรูปแบบการทำงานของการรหัสเช่นนี้ ทำให้ต้องถือกุญแจลับระหว่างผู้รับแต่ละกลุ่มเป็นจำนวนมาก เป็นการเพิ่มความยุ่งยากในการเก็บรักษากุญแจ และเพิ่มโอกาสการถูกลักลอบของกุญแจจากการทำงานร่วมกับหลายกลุ่มด้วยเช่นกัน

2.1.2 การเข้ารหัสแบบอสมมาตร (Asymmetric Key Encryption)

การเข้ารหัสแบบนี้ใช้กุญแจสองตัวเพื่อทำงานตัวหนึ่งใช้ในการเข้ารหัส และอีกตัวหนึ่งใช้ในการถอดรหัสข้อมูลที่เข้ารหัสมาโดยกุญแจตัวใช้ในการเข้ารหัสมักเรียกว่า กุญแจสาธารณะ (Public Key) และกุญแจที่มักใช้ในการถอดรหัสมักเรียกว่า กุญแจส่วนตัว (Private key) ในการถอดรหัสข้อมูลนั้น กุญแจสาธารณะนี้สามารถส่งมอบให้กับผู้อื่นที่ต้องการติดต่อด้วย หรือแม้กระทั่งวางไว้บนเว็บไซต์เพื่อให้ผู้อื่นสามารถดาวน์โหลดไปใช้งานได้สำหรับกุญแจส่วนตัวนั้นเก็บไว้กับผู้เป็นเจ้าของกุญแจส่วนตัว และห้ามเปิดเผย (บรรจง หะรังสี. 2547) ดังรูปที่ 2.3



รูปที่ 2.3 การเข้ารหัสแบบอสมมาตร (Anonymous. 2010)

ข้อเสียของการเข้ารหัสแบบอสมมาตร คือ การเข้ารหัส และถอดรหัสใช้เวลาในการทำงานมากกว่าการเข้ารหัสแบบอสมมาตร เนื่องจากกระบวนการที่ใช้ในการทำงานมีความซับซ้อนกว่า และหากกุญแจลับที่ใช้เข้ารหัสลับมีความยาวน้อยเกินไป อาจทำให้ผู้ไม่หวังดีที่ต้องการข้อมูลดังกล่าว ใช้วิธีการคำนวณหากุญแจอีกตัว และถอดรหัสข้อมูลออกมาโดยใช้เวลาไม่นานได้ ความปลอดภัยของการเข้ารหัสชนิดนี้จึงขึ้นอยู่กับความยาวของคู่กุญแจที่ใช้ในการเข้ารหัส ต้องมีความยาวมากพอที่ทำให้ผู้ไม่หวังดีต้องใช้เวลานานจึงจะสามารถถอดรหัสได้ และต้องมีความยาวของกุญแจไม่มากจนเกินไป เพราะจะทำให้ต้องใช้เวลาในการเข้ารหัส และถอดรหัสนานเช่นเดียวกัน การเข้ารหัสแบบอสมมาตรที่ได้รับความนิยม เช่น RSA (Ron Rivest- Adi Shamir- Len Adleman), DSS (Digital Signature Standard), SET (Secure Electronic Transaction) เป็นต้น

2.2 คุณสมบัติพื้นฐานของระบบความปลอดภัยข้อมูล

การเข้ารหัสลับข้อมูล มีจุดมุ่งหมายเพื่อทำให้ข้อมูลดังกล่าวปลอดภัยจากบุคคลที่ 3 ซึ่งประกอบด้วยคุณสมบัติพื้นฐานดังต่อไปนี้

2.2.1 การรักษาความลับของข้อมูล (Confidentiality)

การเก็บข้อมูลไว้เป็นความลับ เป็นการทำให้ข้อมูลที่ผู้ส่งไม่ต้องการให้บุคคลที่ลักลอบเปิดอ่าน หรือดักจับข้อมูลระหว่างส่งไปยังปลายทางสามารถเข้าถึง หรือทำความเข้าใจกับข้อมูลดังกล่าวได้ โดยการเข้ารหัสข้อมูลก่อนส่ง และมีเฉพาะบุคคลปลายทางที่มีกุญแจที่ถูกต้องเท่านั้น ที่สามารถทำความเข้าใจกับข้อมูลดังกล่าวโดยการถอดรหัส

2.2.2 การรักษาความถูกต้องของข้อมูล (Integrity)

การรักษาความสมบูรณ์ และความถูกต้องของข้อมูล ผู้รับปลายทางต้องได้รับข้อมูลที่ถูกต้องครบถ้วนเช่นเดียวกับต้นฉบับที่ผู้ส่งส่งมา แต่เนื่องจากข้อมูลที่ส่งระหว่างผู้ส่ง และผู้รับ ต้องอาศัยช่องทางในการรับ-ส่ง ทำให้ช่วงเวลาที่ข้อมูลเดินทางมีโอกาสเกิดการลักลอบข้อมูล หรือเปลี่ยนแปลงข้อมูลเกิดขึ้น ทำให้ข้อมูลที่ปลายทางได้รับเป็นข้อมูลที่ผิด ไม่ถูกต้องสมบูรณ์เช่นเดียวกับข้อมูลต้นฉบับ การรักษาความถูกต้องของข้อมูลจึงเป็นสิ่งที่สำคัญหลักอย่างหนึ่งของระบบรักษาความปลอดภัยของข้อมูล

2.2.3 การระบุตัวตน (Authentication)

การระบุตัวตนเป็นสิ่งสำคัญอีกประการของการรักษาความลับของข้อมูล เนื่องจากเป็นสิ่งที่ทำให้ให้ผู้รับ และผู้ส่งมั่นใจว่าอีกฝ่ายที่ตนติดต่ออยู่เป็นบุคคลดังกล่าวจริง ไม่ใช่บุคคลอื่นที่ปลอมแปลงมา

2.2.4 การทำให้ไม่สามารถปฏิเสธได้ (Non-Repudiation)

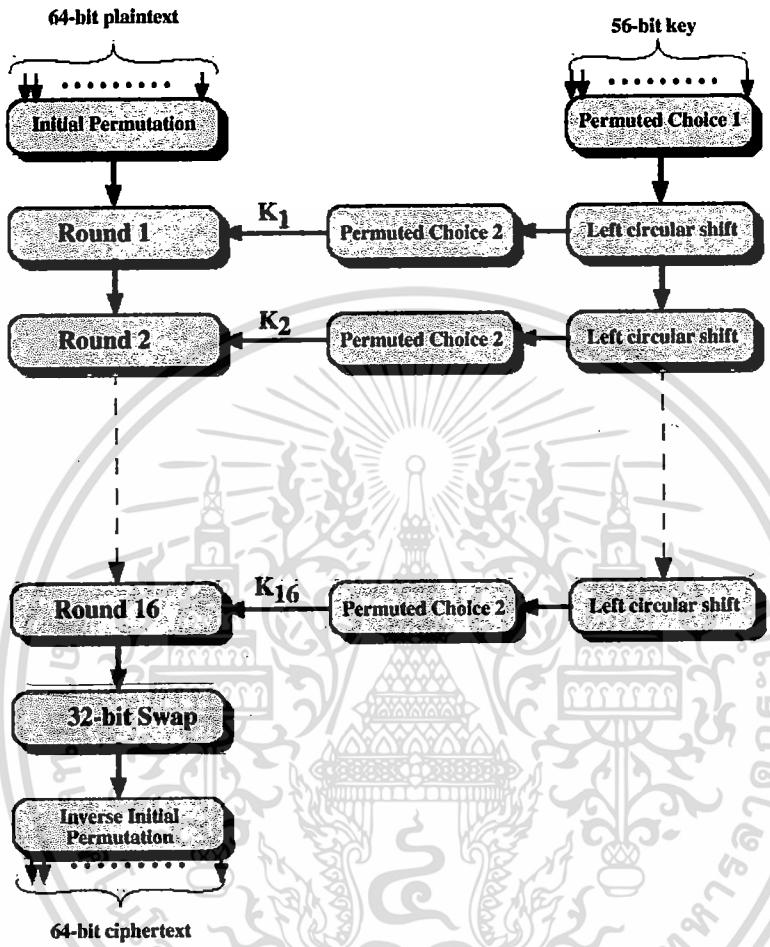
การที่ผู้ส่ง ส่งข้อมูลออกไปให้กับผู้รับ แล้วผู้ส่งไม่สามารถปฏิเสธได้ว่า ข้อมูลดังกล่าวถูกส่งโดยตน เช่นเดียวกับผู้รับ ที่ได้รับข้อมูลดังกล่าวจากผู้ส่งแล้ว ไม่สามารถปฏิเสธได้ว่าตนเป็นผู้รับ จากคุณสมบัติดังกล่าว ทำให้การสื่อสารสามารถยืนยันได้ว่า ใครคือผู้รับและผู้ส่งที่แท้จริง

2.3 อัลกอริทึมของวิทยาการเข้ารหัสลับข้อมูล (Cryptography Algorithms)

2.3.1 DES (Data Encryption Standard) (ธนา หงษ์สุวรรณ. 2547)

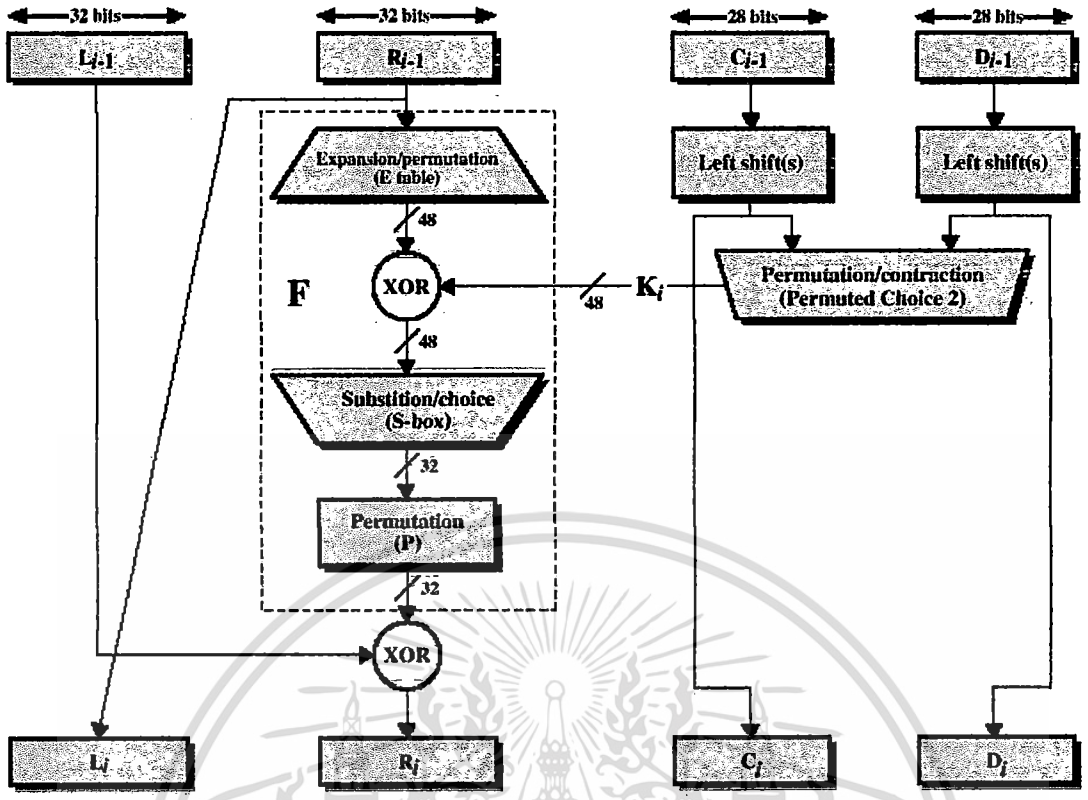
DES เป็นอัลกอริทึมแบบ Block Cipher ที่มีการใช้งานอย่างแพร่หลาย โดย DES เป็นมาตรฐานของ NIST (National Institute of Standard and Technology) ประกาศใช้งานในปี 1977 ใช้ชื่อรหัสว่า FIPS PUB 64 (Federal Information Processing Standard 46) และในปี 1994 ได้

ปรับปรุงมาตรฐานเป็น FIPS PUB 46-2 โดยอัลกอริทึมที่ใช้รู้จักกันในชื่อของ DEA (Data Encryption Algorithm)



รูปที่ 2.4 การทำงานของอัลกอริทึม DES (ธนา หงษ์สุวรรณ, 2547)

จากรูปที่ 2.4 DES จะใช้บล็อกข้อมูลขนาด 64 บิต และใช้กุญแจขนาด 56 บิต โดยหากข้อมูลมีขนาดใหญ่กว่า 64 บิต ก็จะแบ่งออกเป็นบล็อกละ 64 โดยแบ่งออกเป็น 3 ช่วงย่อย โดยช่วงแรกจะเป็นการนำเอาบล็อกข้อมูลมาผ่านการสลับบิตขั้นต้น (Initial Permutation) จากนั้นจะเข้าสู่ช่วงที่ 2 ทำงานเป็นรอบโดยทั้งสิ้นจำนวน 16 ครั้ง และช่วงสุดท้าย จะประกอบด้วยการสลับกลุ่มข้อมูล 32 บิตซ้ายและขวา จากนั้นก็จะนำมาผ่านการสลับบิตย้อนกลับ (Reverse Initial Permutaion) อีกครั้ง ก็จะได้ออกมาเป็น Ciphertext ที่มีความยาวเท่ากับ Plaintext ที่เข้าไป คือ 64 บิต



รูปที่ 2.5 รายละเอียดการเข้ารหัสแต่ละรอบ (ธนา หงษ์สุวรรณ, 2547)

จากรูปที่ 2.5 จะเห็นได้ว่าในแต่ละรอบการทำงานนั้น จะมีการแบ่งข้อมูลขนาด 64 บิตที่ได้จากผลของการทำงานในรอบก่อนหน้าออกเป็นข้อมูล 32 บิต 2 ชุด โดยจะเรียกว่าชุด L และชุด R โดยสามารถเขียนเป็นสมการของการสร้างข้อมูลชุด L และ R ในรอบที่ I ได้ดังสมการ 2.1

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K1) \qquad (2.1)$$

สำหรับฟังก์ชัน F นั้นเป็นฟังก์ชันที่มีทั้งการทำงานในแบบที่มีการสลับบิต (Permutation) และการแทนที่ (Substation) โดยผ่านทาง E Table และ S-BOX โดย E Table จะเป็นการสลับบิตในแบบที่มีการขยายความยาวด้วย จากนั้นจะนำผลลัพธ์ที่ขยายเป็น 48 บิตไป XOR กับคีย์ย่อย จากนั้นเมื่อผ่าน S-BOX แล้วจะถูกลดความยาวลงเหลือ 32 บิตเท่าเดิม และนำไปผ่านฟังก์ชันสลับบิต P อีกครั้ง

ในการพิจารณาถึงความแข็งแกร่งของ DES นั้น จะพิจารณาใน 2 ด้าน คือ ด้านของตัวอัลกอริทึมเอง และด้านความยาวของกุญแจ สำหรับเรื่องของอัลกอริทึมนั้น หลังจากที่ DES ได้ประกาศใช้ออกมา ก็ได้มีผู้คนมากมายพยายามศึกษา และหาจุดอ่อนของ DES จนกล่าวได้ว่า DES เป็นอัลกอริทึมการเข้ารหัสที่มีผู้ศึกษาค้นคว้ามากที่สุดอย่างหนึ่ง

2.3.2 RSA (Rivest-Shamir-Adleman) (Schneier. 1996; นิรนาม. 2551)

การเข้ารหัสแบบ RSA เป็นอัลกอริทึมการเข้ารหัสแบบกุญแจอสมมาตร ในการเข้ารหัสโดยใช้ความรู้เรื่องเลขคณิตมอดุลาร์ (Modular) เข้ามาช่วยในการคำนวณ การเข้ารหัสแบบ RSA เป็นอัลกอริทึมที่ถูกอธิบายเมื่อ ค.ศ. 1978 โดย รอน ริเวสต์ (Ron Rivest), อาดี ชามีร์ (Adi Shamir) และเล็น เอเดิลแมน (Len Adleman) ที่ MIT โดยที่ RSA นั้นเป็นตัวย่อมาจากนามสกุลของทั้ง 3 คน (Rivest-Shamir-Adleman) การเข้ารหัสแบบ RSA ได้จดสิทธิบัตรโดยสถาบัน MIT ในสหรัฐอเมริกาเมื่อปี พ.ศ. 2526 และได้สิ้นสุดลงเมื่อปี พ.ศ. 2543 เพราะเป็นผลงานที่เคยถูกตีพิมพ์เผยแพร่แล้วก่อนที่จะจดสิทธิบัตร

การเข้ารหัสแบบกุญแจอสมมาตร (Public-key cryptography) เป็นการเข้ารหัสที่นิยมใช้กันอย่างแพร่หลายในการทำธุรกรรมอิเล็กทรอนิกส์ เช่นการยืนยันตัวตนด้วยระบบลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) และการค้าผ่านอินเตอร์เน็ต (E-Commerce) โดยการเข้ารหัสจะต้องมีกุญแจสาธารณะ และกุญแจส่วนตัวซึ่งสร้างจากตัวเลขที่สุ่มขึ้นมา และนำมาผ่านขั้นตอนของ RSAโดยกุญแจสาธารณะเป็นตัวที่สามารถเผยแพร่และใช้ร่วมกันได้ แต่กุญแจส่วนตัวจะมีอยู่เฉพาะที่ผู้รับสารเท่านั้น หรือเป็นการเข้ารหัสที่แต่ละคนสามารถใช้กุญแจสาธารณะเดียวกันได้ แต่ในการถอดรหัสออกมาจะขึ้นอยู่กับกุญแจส่วนตัวของผู้รับสารที่จะถอดรหัส

ความยากของการถอดรหัส RSA อยู่ที่การแยกตัวประกอบของเลขที่มีขนาดใหญ่มากๆ เนื่องจากกุญแจของระบบถูกสร้างขึ้นจากจำนวนเฉพาะ 2 จำนวน ดังสมการที่ 2.2

$$n = p \times q \tag{2.2}$$

หาค่ากุญแจสาธารณะ โดยใช้ e แทนจำนวนเฉพาะใดๆที่มีค่าน้อยกว่า (p-1)(q-1) และไม่เป็นตัวประกอบของ (p-1)(q-1) นำค่ากุญแจสาธารณะ หรือ e ที่ได้ คำนวณหาค่ากุญแจส่วนตัว หรือ d โดยใช้สมการที่ 2.3

$$d \times e = 1 \bmod [(p-1)(q-1)] \tag{2.3}$$

เมื่อต้องการเข้ารหัสลับข้อความ อาศัยสมการที่ 2.4 โดยกำหนดให้ c คือ ข้อความที่ถูกเข้ารหัสแล้ว และ m อข้อความที่ยังไม่ถูกเข้ารหัส

$$c = m^e \bmod n \tag{2.4}$$

กรณีต้องการถอดรหัสข้อความ c ให้เป็นข้อความ m อาศัยสมการที่ 2.5

$$m = c^d \bmod n \qquad (2.5)$$

ความแตกต่างระหว่างการใช้ RSA สำหรับการเซ็นลายเซ็นดิจิตอล และการเข้ารหัสลับ คือ

- กรณีใช้สำหรับเซ็นลายเซ็นดิจิตอล

สมมติว่าผู้ส่งต้องการส่งข้อความ m ให้กับผู้รับ โดยผู้รับ B ต้องการความมั่นใจว่าข้อความนี้ถูกส่งโดยผู้ส่ง จริง ผู้ส่งจึงสร้างลายเซ็นดิจิตอล s ขึ้นจากสมการ $s = m^d \bmod n$ โดยที่ d คือกุญแจส่วนตัวของผู้ส่ง จากนั้นผู้ส่ง ส่งข้อความ m และ s ให้ผู้รับ ผู้รับใช้ s ที่ได้จากข้อมูลแก้สมการ $m = s^d \bmod n$ โดยที่ e และ n เป็นกุญแจสาธาณะของผู้ส่ง ซึ่งหากผู้รับเปรียบเทียบข้อความ m ที่ได้รับแล้วเหมือนกัน แสดงว่าผู้ส่ง เป็นผู้ส่งข้อความนี้จริง

- กรณีใช้สำหรับการเข้ารหัสลับ

สมมติว่านาย A ต้องการส่งข้อความ $\bar{m}$ ให้กับนาย B นาย A จึงเข้ารหัสลับข้อความ $\bar{m}$ จากสมการ $c = m^e \bmod n$ โดย e และ n เป็นกุญแจสาธารณะของนาย B จากนั้นนาย A ส่งข้อความเข้ารหัสลับ c ที่ได้จากสมการให้นาย B นาย B ใช้กุญแจส่วนตัวของตนถอดรหัสลับข้อความ c ที่ได้รับโดยใช้สมการ $m = c^d \bmod n$

2.3.3 MD5 (Message Digest algorithm 5) (Schneier. 1996)

MD5 เป็นฟังก์ชันแฮชทางเดียวรูปแบบหนึ่ง (One-Way Hash Function) ถูกคิดค้นขึ้นในปี 1991 โดย Rivest หนึ่งในผู้คิดค้นการเข้ารหัสแบบ RSA มีจุดประสงค์เพื่อแปลงข้อมูลที่มีความยาวมากๆ ให้อยู่ในอีกรูปแบบหนึ่งที่มีขนาดคงที่ขนาด 128 บิต โดยผลลัพธ์ที่ได้จะเป็นค่าแฮชซึ่งอาจเรียกว่า Message Digest หรือ Fingerprint

การทำงานของ MD5 มีขั้นตอนดังนี้

1. ข้อมูลที่มีความยาวหารด้วย 512 แล้วเหลือเศษไม่เท่ากับ 448 (หรือเหลืออีก 64 จึงจะหาร 512 บิตลงตัว) จะถูกต่อท้ายด้วย Padding bit เพื่อให้ข้อมูลมีความยาวมากพอที่จะหารด้วย 512 ลงตัว โดย Padding bit คือ บิตขนาด 1 บิต มีค่า 1 และตามด้วยบิตที่มีค่า 0 จำนวนตามต้องการ

2. หลังจากเติม Padding bit จนข้อมูลมีความยาวมากพอจะหารด้วย 512 แล้วเหลือเศษ 448 แล้ว ข้อมูลจะถูกต่อท้ายด้วยบิตบอกความยาวขนาด 64 บิต ทำให้ข้อมูลที่ได้ เป็นข้อมูลคงที่ขนาด 512 บิต

3. ตั้งค่าเริ่มต้นตัวแปร 4 ตัว ขนาดตัวละ 32 บิต (A, B, C, D) มีค่าเริ่มต้นในเลขฐาน 16 และคัดลอกไปตัวแปร A, B, C, D ตามลำดับ

4. เริ่มรอบการทำงาน โดยจำนวนรอบขึ้นอยู่กับจำนวนบล็อกของข้อมูลขนาด 512 บิต รอบการทำงานหลักของ MD5 มี 4 รอบ แต่ละรอบจะถูกใช้ในการคำนวณที่ต่างกัน 16 ครั้ง การคำนวณแต่ละครั้งใช้ฟังก์ชันแบบไม่เชิงเส้น โดยมีข้อมูลขาเข้าเป็น 3 ค่า จาก A, B, C, D และผลลัพธ์ถูกเพิ่มไปยังตัวแปรที่ 4 หลังจากนั้นจะมีการหมุนผลลัพธ์ไปทางขวาตามจำนวนบิตของตัวแปร และเพิ่มให้กับ A, B, C หรือ D ตัวใดตัวหนึ่ง สุดท้ายผลลัพธ์ก็จะแทนที่ตัวแปรตัวหนึ่ง

2.4 โพรโตคอลของวิทยาการเข้ารหัสข้อมูล (Cryptography Protocols)

2.4.1 Authentication

การพิสูจน์ตัวจริงระหว่างผู้ใช้กับธนาคาร ใช้หมายเลขบัตรประจำตัวประชาชน และรหัสลับ (Password) เป็นตัวพิสูจน์ตัวตน เพื่อให้ธนาคารมั่นใจได้ว่า ผู้ที่กำลังจะเข้าใช้งานระบบ คือใคร

การพิสูจน์เพื่อให้ร้านค้ามั่นใจได้ว่า เงินสดดิจิตอลที่ลูกค้านำมาใช้ เป็นเงินสดที่ออกโดยธนาคารอย่างถูกต้อง ใช้โพรโตคอลการเข้ารหัสลับแบบกุญแจสาธารณะ โดยเริ่มแรกซอฟต์แวร์ของร้านค้า จะมีกุญแจสาธารณะของธนาคารในระบบอยู่แล้ว โดยธนาคารจะใช้กุญแจส่วนตัวของตนเซ็นลงในเงินสดดิจิตอล

2.4.2 Secret Splitting

เป็นโพรโตคอลที่มีการทำงานโดยการแบ่งข้อมูลออกเป็นส่วนๆ โดยแต่ละส่วนไม่สามารถบอกความหมายของข้อมูลได้ นอกจากจะนำข้อมูลทุกส่วนที่ถูกแบ่งออกกลับมารวมกัน จึงจะสามารถแปลงกลับมาเป็นข้อมูลต้นฉบับที่สามารถทำความเข้าใจได้ จุดประสงค์ของโพรโตคอลนี้ คือ การแบ่งข้อความออกเป็นส่วนๆ แยกเก็บไว้ที่บุคคลแต่ละฝ่าย แต่ละฝ่ายไม่สามารถอ่าน หรือทำความเข้าใจข้อมูลส่วนที่ตนเองถือได้ จนกว่าจะนำข้อมูลทุกส่วนมารวมกัน โดยธนาคารเป็นผู้แบ่งข้อมูล ตัวอย่างขั้นตอนการแบ่งข้อมูลออกเป็น 2 ส่วน มีขั้นตอนดังนี้

1. ธนาคารสร้างข้อความสุ่ม R ที่มีความยาวเท่ากับข้อความ M
2. ธนาคาร Exclusive OR (XOR) ข้อความ M กับข้อความสุ่ม R ได้ผลลัพธ์เป็น Z ดังสมการ 2.6

$$M \oplus R = Z \tag{2.6}$$

3. ธนาคารให้ R กับคนหนึ่ง และ Z กับอีกคน
4. ผู้ใช้ทั้ง 2 สร้างข้อความ M กลับได้จากสมการ 2.7

$$M \oplus R = Z \qquad (2.7)$$

โพรโตคอลนี้สามารถประยุกต์ใช้กับผู้ใช้มากกว่า 2 คน โดยการแตกข้อความสุ่มเพิ่มเท่ากับจำนวนผู้ใช้ลบหนึ่ง เพื่อนำไป XOR กับข้อความต้นฉบับ เช่น มีผู้ใช้ 5 คน ก็ทำการแตกข้อความสุ่มออกเป็น 4 ส่วน เป็นต้น และเข้าสู่ขั้นตอนเช่นเดียวกับที่ได้ยกตัวอย่างการมีผู้ใช้ 2 คน

2.4.3 Bit Commitment (Schneier. 1996)

เป็นโพรโตคอลที่ใช้สำหรับผูกมัดตัวเองกับข้อความ เพื่อให้ผู้ที่ติดต่อด้วยมั่นใจว่าข้อความจะไม่ถูกเปลี่ยนแปลงหลังจากผู้ใช้ได้ผ่านกระบวนการทำงานของโพรโตคอลนี้แล้ว โดยโพรโตคอล Bit Commitment ที่ใช้การเข้ารหัสแบบสมมาตร (Symmetric Encryption) มีขั้นตอนการทำงานดังนี้

1. ผู้ใช้ A สร้างข้อความสุ่ม R ส่งให้ผู้ใช้ B
2. ผู้ใช้ B สร้างข้อความที่ประกอบด้วยบิตข้อมูล x ที่ผู้ใช้ B ต้องการจะผูกมัดตัวเอง และข้อความสุ่ม r ทำการเข้ารหัสลับด้วยกุญแจ k ได้ $E_k(r, x)$ แล้วส่งข้อความนี้ให้ผู้ใช้ A จนถึงตรงนี้ผู้ใช้ A จะไม่สามารถถอดรหัสข้อความนี้ได้ ทำให้ค่า x ยังคงเป็นความลับ
3. ผู้ใช้ B ส่งกุญแจลับให้ผู้ใช้ A
4. ผู้ใช้ A ทำการถอดรหัส สามารถทราบค่า x และตรวจสอบความถูกต้องได้จากค่า r

โพรโตคอล Bit Commitment แบบฟังก์ชันทางเดียว มีขั้นตอนการทำงานดังนี้

1. ผู้ใช้สร้างข้อความสุ่ม R1 และ R2
2. ผู้ใช้สร้างข้อความสุ่ม R1, R2 และบิตข้อมูล x ที่ต้องการผูกมัด
3. ผู้ใช้คำนวณค่าที่ได้จากฟังก์ชันแบบทางเดียวของข้อความ และส่งไปให้ผู้รับพร้อมกับค่าข้อความสุ่มค่าใดค่าหนึ่ง เช่น H(R1, R2, x), R2 เป็นต้น ในขั้นตอนนี้ผู้ใช้ได้ผูกมัดตัวเองกับบิตข้อมูล และการใช้ฟังก์ชันแบบทางเดียวในข้อ 3 เพื่อป้องกันผู้รับคำนวณกลับเพื่อหาค่า x
4. ผู้ใช้ส่งข้อความเดิม (R1, R2, x) ให้ผู้รับ
5. ผู้รับคำนวณค่าฟังก์ชันแบบทางเดียวจากข้อความที่ได้รับ และเปรียบเทียบค่าดังกล่าวกับ R2 ที่ได้รับจากข้อ 3 ถ้าเหมือนกันแสดงว่าบิตข้อมูลเป็นข้อความเดิมที่เก็บเอาไว้

โพรโตคอล Bit Commitment ที่ใช้ฟังก์ชันแบบทางเดียวมีข้อดี เหมาะสมกับการใช้งานมากกว่าแบบ Symmetric Encryption คือ ผู้ที่ต้องการผูกมัดตัวเองกับข้อความไม่ต้องอาศัยข้อความสุ่มจากผู้รับ ผู้ใช้เพียงแค่ส่งข้อความที่ผูกมัดกับข้อความสุ่มตัวหนึ่งให้กับผู้รับ ข้อความสุ่มจากผู้รับไม่มีความจำเป็น เพราะการผูกมัดตัวเองของผู้ใช้โดยใช้ฟังก์ชันแบบทางเดียว ผู้ใช้ไม่สามารถ

คำนวณข้อความ (R1', R2', x') ซึ่ง (R1', R2', x') = (R1, R2, x) เนื่องจากการส่ง R2 ไปยังผู้รับ เป็นการผูกมัดตัวเองกับ x ถ้าผู้ใช้ไม่เก็บ R1 ไว้เป็นความลับ ผู้รับจะสามารถคำนวณ H(R1, R2, x) และ H(R1, R2, x') และเปรียบเทียบกับที่ได้รับจากผู้ส่ง ก็จะทราบบิตข้อมูล x (Schneier. 1996)

2.4.4 Blind Signature

เป็นเทคนิคการลงลายมือชื่อลับที่ผู้ลงลายมือชื่อตั้งใจลงลายมือชื่อตามคำขอเท่านั้น โดยไม่จำเป็นต้องรู้ว่าตนลงลายมือชื่อบนข้อมูลใด หรือลายมือชื่อที่ได้มีลักษณะเป็นอย่างไร เทคนิคนี้พัฒนาขึ้นโดย David Chuam ในปี 1982 เป็นวิธีการซ่อนข้อมูลไม่ให้ผู้ลงลายมือชื่อเห็นข้อมูลต้นฉบับซึ่งเป็นพื้นฐานสำคัญสำหรับระบบเงินสดดิจิตอลต่อมา ตัวอย่างของ Blind Signature บน RSA Signature Scheme มีดังนี้

ลูกค้าเลือก Blind Factor r อย่างสุ่ม และไม่ขึ้นกับข้อความต้นฉบับ แล้วคำนวณค่า Blind Message ตามสมการ 2.8 จากนั้นส่งค่า b ให้ธนาคาร

$$b = x^{*}r^{e} \pmod{n} \tag{2.8}$$

เมื่อ (e,n)เป็น กุญแจสาธารณะ และเมื่อธนาคารได้รับ b จึงทำการลงลายมือชื่อดิจิตอลด้วยกุญแจส่วนตัว d ตามสมการ 2.9 แล้วส่งค่า b^{d} กลับไปให้ลูกค้า

$$B^{d} = (x^{*}r^{e})^{d} = (x^{d})^{*}(r^{(e^{*}d)}) = r^{*}x^{d} \pmod{n} \tag{2.9}$$

ลูกค้าคำนวณค่า Signed Message ตามสมการ 2.9 จะได้ข้อมูลเดิมที่ลงลายมือชื่อธนาคาร

$$(r^{*}x^{d})|r = x^{d} \pmod{n} \tag{2.10}$$

จากสมการ 2.10 จะเห็นว่าค่า r เป็นเลขสุ่ม ดังนั้นธนาคารไม่สามารถหาค่า x จากข้อมูลที่ลูกค้าส่งให้ได้ธนาคารจึงไม่สามารถเชื่อมข้อมูลของลูกค้ากับเงินสดดิจิตอลที่ลงลายมือชื่อไปได้ เมื่อลูกค้านำเงินสดดิจิตอลไปใช้ ลายมือชื่อบนเงินสดดิจิตอลทำให้ธนาคารสามารถใช้ตรวจสอบความถูกต้องได้ แต่ไม่สามารถรู้ได้ว่าใครเป็นเจ้าของเงินสดดิจิตอล

Blind Signature เป็นวิธีการสร้างความเป็นส่วนตัวในด้านข้อมูลของระบบอิเล็กทรอนิกส์ในปัจจุบัน หลังจากการคิดค้นของ Chuam แล้วได้มีงานวิจัยเกี่ยวกับ Blind Signature บนระบบลายมือชื่อดิจิตอลอื่น ๆ ออกมาภายหลัง ระบบเงินสดดิจิตอลที่ทำงานร่วมกับสมาร์ทการ์ด (Schneier. 1996)

2.5 ระบบเงินสดดิจิตอล (Digital Cash) (Schneier. 1996; Chuam, Fiat, Naor. 1990; Chuam. 1985)

ระบบเงินสดดิจิตอล หรือเรียกอีกอย่างว่า Digital Cash หมายถึงระบบการชำระเงินผ่านอุปกรณ์อิเล็กทรอนิกส์ที่สร้างขึ้นจากข้อมูล หรือข้อความอิเล็กทรอนิกส์เพื่อใช้แทนเงินสด โดยใช้อุปกรณ์อิเล็กทรอนิกส์ เช่น บัตรสมาร์ทการ์ดในการถ่ายโอนข้อมูลอิเล็กทรอนิกส์ในการชำระเงิน โดยที่ค่าของเงินจะเป็นเพียงชุดข้อมูลดิจิตอลเท่านั้น

ธนาคารเป็นผู้ทำหน้าที่สร้างชุดข้อมูลเหล่านี้ และตัดเงินในบัญชีผู้ใช้ออกเป็นจำนวนเงินเท่ากับมูลค่าของชุดข้อมูลที่สร้าง ในการสร้างเงินสดดิจิตอลนั้นทางธนาคารจะตรวจสอบข้อมูลของจำนวนเงิน พร้อมกับเพิ่มรายละเอียดในชุดข้อมูลของเงินสดดิจิตอลว่าสามารถนำเงินสดดิจิตอลไปชำระค่าสินค้า หรือบริการได้ ลูกค้าสามารถซื้อสินค้าที่ร้านค้าได้โดยการส่งชุดข้อมูลดังกล่าวให้ร้านค้า ทางร้านค้าจะนำชุดข้อมูลไปตรวจสอบว่าเป็นเงินที่ออกโดยธนาคารจริงหรือไม่ ถ้าทุกอย่างถูกต้องเรียบร้อย ลูกค้าจะสามารถใช้เงินสดดิจิตอลดังกล่าวชำระกับร้านได้ตามปกติ

ในปัจจุบันระบบการจ่ายเงินแบบดิจิตอลถูกแบ่งออกเป็น 2 ประเภทใหญ่ๆ ได้แก่ Account-based systems และ Token-based systems

1. Account-based systems เป็นระบบที่สามารถระบุตัวตนผู้ใช้จ่าย หรือทำ Transactions ได้ โดยใช้บัญชี (Account) เป็นสื่อการอ้างถึงมูลค่าของเงินของแต่ละบุคคล ยกตัวอย่าง เช่น เช็ค, บัตรเครดิต เป็นต้น

2. Token-based systems ระบบที่ไม่สามารถระบุตัวตนของผู้ใช้จ่าย หรือทำ Transaction ได้ โดยใช้ตั๋ว (Token) เป็นตัวแทนการอ้างถึงมูลค่าของเงิน เช่น เงินสด, บัตรเติมเงินโทรศัพท์, สแตมป์ เป็นต้น

และหากแบ่งตามลักษะการทำงานของระบบ สามารถแบ่งเป็น 2 ประเภทได้เช่นกัน คือ

1. ระบบเงินสดดิจิตอลแบบออนไลน์ (On-line Electronic Cash System) คือ ระบบการชำระเงินที่มีการติดต่อสื่อสารแบบออนไลน์ระหว่างร้านค้ากับธนาคารในขณะที่ทำขั้นตอนการชำระเงิน ร้านค้าสามารถทำการตรวจสอบเงินสดดิจิตอลของลูกค้ากับธนาคารได้ว่าเป็นเงินสดดิจิตอลที่ธนาคารออกให้จริงหรือไม่ ธนาคารต้องเก็บข้อมูลของเงินสดดิจิตอลโดยใช้ฐานข้อมูลที่มีการปรับปรุงข้อมูลให้ทันสมัยอยู่ตลอดเวลา และการตรวจสอบต้องเป็นลำดับ ซึ่งการดำเนินการดังกล่าวมีค่าใช้จ่ายสูง ดังนั้นจึงเหมาะที่จะใช้กับการชำระเงินวงเงินสูงจึงคุ้มทุน แต่มีข้อดีคือเป็นระบบที่ร้านค้ามั่นใจว่าได้เงินสดดิจิตอลที่มีมูลค่าแน่นอน

2. ระบบเงินสดดิจิตอลแบบออฟไลน์ (Off-line Electronic Cash System) คือ ระบบการชำระเงินที่ไม่มีการติดต่อสื่อสารระหว่างร้านค้ากับธนาคารในขณะขั้นตอนที่ทำการชำระเงิน ไม่มี

การตรวจสอบเงินสดดิจิตอลของลูกค้ากับธนาคาร ระบบนี้เหมาะสำหรับการชำระเงินในวงเงินต่ำ ช่วยลดต้นทุนในการดำเนินการ ตัวอย่างเช่น ระบบการชำระเงินบนอินเตอร์เนต ร้านค้าสามารถตรวจสอบเงินสดดิจิตอลได้เอง ไม่ต้องตรวจสอบผ่านธนาคาร ทำให้ระบบทำงานได้เร็วขึ้น

คนทั่วไปชอบการใช้เงินในลักษณะของเงินสด เนื่องจากง่ายต่อการใช้ เพราะสามารถใช้เงินสดแทนมูลค่าสินค้า หรือบริการได้ทันที โดยที่ไม่ต้องการ Third-Party อย่างเช่นธนาคารในการรับรองมูลค่าของเงินที่ใช้ ในระหว่างที่ทำการแลกเปลี่ยนสินค้าหรือบริการกับธนบัตร แต่การถือเงินสดมีความเสี่ยงต่อการถูกโจรกรรม เนื่องจากคนภายนอกสามารถทราบมูลค่าของเงินที่ถือได้ ดังนั้นหากจำเป็นต้องถือเงินมากๆ เพื่อซื้อสินค้า ย่อมเป็นการเพิ่มความเสี่ยงต่อตัวผู้ถือด้วยเช่นกัน

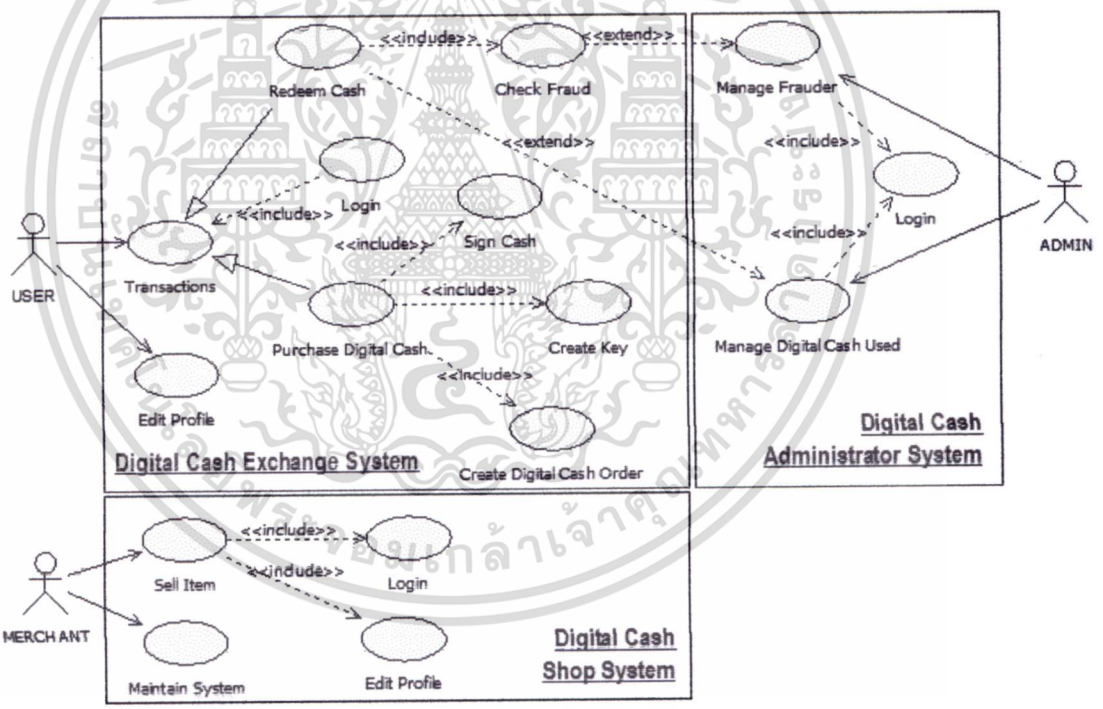
บัตรเครดิตเข้ามามีส่วนช่วยลดความเสี่ยงที่เกิดขึ้นจากการใช้เงินสด แต่จะเสียความเป็นส่วนตัวไป ซึ่งจากการแพร่หลายของอินเตอร์เน็ต ส่งผลให้ความต้องการ และคาดหวังในประสิทธิภาพของระบบจ่ายเงินอิเล็กทรอนิกส์นี้มีเพิ่มมากขึ้นไปด้วย

เนื่องจากการไม่เปิดเผยชื่อของการชำระเงินมักจะเกี่ยวข้องกับการไม่เปิดเผยชื่อของเงินสดกระดาษ, ระบบการจ่ายเงินอิเล็กทรอนิกส์แบบ Token-based จึงถูกเรียกว่า "ระบบเงินสดดิจิตอล" (Digital Cash, Electronic Cash, e-cash, d-cash) Digital cash คือ ทางเลือกหนึ่งที่เป็นทางออกสำหรับทั้งเงินสด และบัตรเครดิตเนื่องจากสามารถให้ความปลอดภัยกว่าการถือเงินสด และให้ความเป็นส่วนตัวมากกว่าระบบบัตรเครดิต ผู้ใช้สามารถใช้เงินสดดิจิตอลใช้จ่ายได้โดยที่ไม่ต้องเกี่ยวข้องกับธนาคารตลอดเวลาการชำระเงิน ซึ่งระบบเงินสดดิจิตอลแบบ Token-based systems เป็นรูปแบบที่นำมาประยุกต์เพื่อพัฒนาเป็นระบบเงินสดดิจิตอลชนิดออฟไลน์ในโครงงาน

บทที่ 3
การออกแบบระบบเงินสดดิจิตอลชนิดออฟไลน์

เมื่อศึกษาวิทยาการเข้ารหัสลับ และเทคโนโลยีที่เกี่ยวข้องกับการพัฒนาระบบเงินสดดิจิตอลชนิดออฟไลน์แล้ว จึงได้ทำการวิเคราะห์ และออกแบบระบบ โดยแสดงรายละเอียดขั้นตอนการทำงานจากการหาความสัมพันธ์ระหว่างสิ่งต่างๆที่เป็นองค์ประกอบของระบบเข้าด้วยกัน ซึ่งแสดงออกในรูปแบบแผนภาพยูสเคส (Use Case Diagram) แสดงขั้นตอนการทำงานของกิจกรรมในส่วนต่างๆของระบบด้วยแผนภาพกิจกรรม (Activity Diagram) และแสดงถึงรูปแบบการเก็บข้อมูล และโครงสร้างของฐานข้อมูลโดยใช้แผนภาพความสัมพันธ์ของเอนทิตี (ER Diagram)

3.1 ภาพรวมของระบบ



รูปที่ 3.1 แผนภาพยูสเคสแสดงภาพรวมของระบบ

จากรูปที่ 3.1 การทำงานของระบบเงินสดดิจิตอลชนิดออฟไลน์ประกอบด้วย 3 ระบบย่อย ได้แก่ ระบบแลกเปลี่ยนเงินสดดิจิตอล (Digital Cash Exchange System), ระบบเงินสดดิจิตอลสำหรับร้านค้า (Digital Cash Shop System) และระบบเงินสดดิจิตอลสำหรับผู้ดูแลระบบ (Digital Cash Administrator System) ซึ่งหน้าที่ของแต่ละระบบเป็นดังต่อไปนี้

3.1.1 ระบบแลกเปลี่ยนเงินสดดิจิตอล (Digital Cash Exchange System)

ระบบแลกเปลี่ยนเงินสดดิจิตอล เป็นระบบที่ใช้ติดต่อกับผู้ใช้ระบบ (User) ทั้งผู้ใช้ที่มีบทบาทเป็นผู้ซื้อ และผู้ใช้ที่มีบทบาทเป็นผู้ขาย มีการทำงานหลักคือ การซื้อเงิน การคืนเงิน และการตรวจสอบทุจริตผู้ใช้งานระบบ โดยออกแบบส่วนติดต่อกับผู้ใช้ของระบบให้มีลักษณะคล้ายกับส่วนติดต่อกับผู้ใช้ของตู้เอทีเอ็ม (ATM) ด้วยแนวคิดที่จะพัฒนาระบบเงินสดดิจิตอลให้เป็นบริการเสริมของธนาคารอีกอย่างหนึ่ง และเพื่อให้เกิดความสะดวกกับผู้ใช้ จึงออกแบบ และตั้งสมมติฐานให้สามารถซื้อเงินสดดิจิตอลได้จากตู้เอทีเอ็ม

ในบทบาทของผู้ซื้อ ผู้ใช้ระบบต้องทำการเปิดบัญชี และสมัครบริการเงินสดดิจิตอลกับเจ้าของธนาคารก่อนเข้าใช้งานระบบ โดยระบบจะทำหน้าที่เปลี่ยนเงินสด (Cash) เป็นเงินสดในรูปแบบดิจิตอล (Digital Cash) ซึ่งในระบบเรียกว่า "การซื้อเงิน" โดยเงินสดดิจิตอลจะมีคุณสมบัติการรักษาความเป็นส่วนตัวเช่นเดียวกับเงินสดธรรมดา แต่อยู่ในรูปแบบไฟล์ข้อมูล และใช้อุปกรณ์เชื่อมต่อในการบันทึกไฟล์เงินสดดิจิตอลดังกล่าว เพื่อนำไปใช้จ่ายที่ร้านค้าต่อไป

ในบทบาทของผู้ขาย ผู้ใช้ระบบต้องทำการเปิดบัญชีกับธนาคารและสมัครบริการเงินสดดิจิตอลกับธนาคารเช่นเดียวกับผู้ซื้อ ซึ่งระบบจะทำหน้าที่เปลี่ยนเงินสดดิจิตอลเป็นเงินสดให้กับผู้ขาย หรือที่ในระบบเรียกว่า "การคืนเงิน หรือขึ้นเงิน" โดยระบบสามารถเลือกรูปแบบการคืนเงินได้ ว่าเป็นการคืนเงิน หรือขึ้นเงินในลักษณะเงินสด หรือโอนเข้าบัญชีของผู้ขึ้นเงิน

ระบบแลกเปลี่ยนเงินสดดิจิตอลนี้สามารถตรวจสอบการทุจริตได้ทั้งขั้นตอนการซื้อเงินและคืนเงิน หรือขึ้นเงิน ซึ่งหากมีการทุจริต ระบบสามารถทราบได้ถึงผู้กระทำผิด

3.1.2 ระบบเงินสดดิจิตอลสำหรับร้านค้า (Digital Cash Shop System)

ระบบเงินสดดิจิตอลสำหรับร้านค้า เป็นส่วนผู้ขายใช้ติดต่อกับผู้ซื้อเพื่อดำเนินการซื้อขายสินค้า โดยใช้เงินสดดิจิตอลแทนเงินสดปกติ โดยระบบฯจะทำงานในลักษณะออฟไลน์ กล่าวคือระบบของร้านค้าจะไม่มีการเชื่อมต่อไปยังธนาคารในระหว่างทำการซื้อขาย และตรวจสอบเงินสดดิจิตอล ซึ่งรายละเอียดการตรวจสอบของระบบจะได้กล่าวให้ทราบในบทต่อไป

เงินสดดิจิตอลที่ได้จากการซื้อขาย จะถูกบันทึกลงในอุปกรณ์บันทึกสำหรับร้านค้า โดยร้านค้าไม่สามารถนำเงินสดดิจิตอลที่ได้ไปใช้ต่อได้ และในส่วนของการทอนเงิน ระบบเงินสดดิจิตอลนี้ไม่มีฟังก์ชันสำหรับการทอนเงินในรูปแบบเงินสดดิจิตอลให้กับผู้ซื้อ โดยหากจำเป็นต้องมีการทอนเงิน ระบบจะทอนเงินสดปกติให้กับผู้ซื้อ เพื่อลดความซับซ้อนของระบบ

3.1.3 ระบบเงินสดดิจิตอลสำหรับผู้ดูแลระบบ (Digital Cash Administrator System)

ระบบเงินสดดิจิตอลสำหรับผู้ดูแลระบบเป็นส่วนที่ติดต่อกับเจ้าหน้าที่ที่ดูแลระบบเงินสดดิจิตอลของธนาคารเท่านั้น โดยระบบจะทำหน้าที่แสดงรายงานเงินสดดิจิตอลใช้แล้ว และรายชื่อผู้กระทำการทุจริต โดยรายชื่อผู้กระทำการทุจริตจะถูกดำเนินการทางกฎหมายจากธนาคารต่อไป

3.2 สมมติฐานของระบบ

1. การซื้อเงิน

- ผู้ใช้งานระบบเงินสดดิจิตอลต้องเปิดบัญชี และสมัครบริการเงินสดดิจิตอลกับธนาคารก่อน จึงจะสามารถใช้งานระบบเงินสดดิจิตอลนี้ได้ โดยระบบนี้อยู่บนสมมติฐานที่ผู้ใช้ทุกคนเปิดบัญชีกับธนาคาร และสมัครบริการเงินสดดิจิตอลของเรียบร้อยแล้ว ระบบจึงไม่มีส่วนการทำงานที่เกี่ยวข้องกับการเปิดบัญชี และสมัครบริการ

- ในการสมัครบริการเงินสดดิจิตอล ธนาคารจะอนุมัติวงเงินสำหรับผู้สมัคร ดังนั้นในการซื้อเงินสดดิจิตอลผู้ใช้จะสามารถซื้อเงินสดดิจิตอลได้สูงสุดตามจำนวนวงเงินที่ได้รับอนุมัติเท่านั้น และเงินในบัญชีที่ผูกกับบริการเงินสดดิจิตอล ต้องมีเงินอยู่เพียงพอกับจำนวนเงินดังกล่าวด้วย ทั้งนี้เพื่อป้องกัน และลดโอกาสการเกิดหนี้สูญจากผู้ใช้ที่ต้องการทุจริต

- ในแต่ละวัน ผู้ใช้สามารถซื้อเงินสดได้ไม่จำกัดจำนวนครั้ง แต่จำนวนรวมของการซื้อเงินสดดิจิตอลในแต่ละวันต้องไม่เกินวงเงินที่ได้รับอนุมัติ

- เงินสดดิจิตอลที่ได้จากระบบจะเป็นเงินสดดิจิตอลจำนวนหนึ่งที่ไม่สามารถแตกเงินได้ ยกตัวอย่างเช่น การนำเงินสดดิจิตอล 100 บาท ซื้อของจำนวน 50 บาท จะไม่สามารถนำสดดิจิตอลที่เหลืออีก 50 ไปใช้ต่อได้ ดังนั้นการซื้อของ 50 บาทนี้ จะได้รับเงินทอนจากร้านค้าในรูปแบบเงินสดจำนวน 50 บาท

- เงินสดดิจิตอลที่ได้จากระบบทุกอันจะมีวันหมดอายุของเงิน เพื่อประโยชน์ในการจัดการกับเงินสดดิจิตอลที่ใช้แล้ว

- ในขั้นตอนการซื้อเงิน ผู้ใช้จะถูกตรวจสอบทุจริต โดยผู้ใช้ที่ตรวจพบการทุจริตหรืออยู่ในสถานะผู้ต้องสงสัยการทุจริตมากกว่า 1 ครั้ง จะไม่สามารถดำเนินการซื้อเงินสดดิจิตอลกับระบบได้ ต้องติดต่อโดยตรงกับธนาคาร

2. การคืนเงิน หรือขึ้นเงิน

- การขึ้นเงินต้องขึ้นเงินเต็มจำนวนเท่านั้น เนื่องจากระบบไม่มีคุณสมบัติการแตกเงิน ยกตัวอย่างเช่น ร้านค้านำเงินสดดิจิตอล 1,000 บาท มาขึ้นเงิน ร้านค้าจะไม่สามารถขึ้นเงินเพียง 500 บาทได้

- ในขั้นตอนการขึ้นเงิน หากตรวจพบการทุจริตโดยร้านค้า หรือผู้ขึ้นเงินนี้เป็นผู้ทุจริตเอง ระบบจะไม่ดำเนินการขึ้นเงินส่วนนั้น และจะเพิ่มข้อมูลร้านค้านี้ลงในฐานข้อมูลผู้ทุจริตของธนาคาร โดยมีสถานะเป็นผู้ต้องสงสัยในการทุจริต

- ในขั้นตอนการขึ้นเงิน หากตรวจพบการทุจริตโดยลูกค้าของร้านค้า เป็นผู้ทุจริต ระบบจะดำเนินการขึ้นเงินส่วนนั้นให้กับร้านค้า หรือผู้ขึ้นเงินตามปกติ โดยจะเพิ่มข้อมูลบุคคลผู้ทุจริตในฐานข้อมูลผู้ทุจริตของธนาคาร โดยมีสถานะเป็นผู้ต้องสงสัยในการทุจริต

3. การซื้อสินค้า

- ผู้ซื้อ และผู้ขายสามารถดำเนินการซื้อขายได้ตามปกติ โดยใช้เงินสดดิจิตอลที่ได้จากธนาคารอย่างถูกต้อง แทนเงินสดธรรมดา

- เงินสดดิจิตอล 1 จำนวน สามารถซื้อสินค้า และบริการได้ไม่จำกัดจำนวนชิ้น แต่ราคารวมของสินค้า หรือบริการนั้น ต้องน้อยกว่า หรือเท่ากับจำนวนเงินของเงินสดดิจิตอลอันนั้น

- ร้านค้าไม่สามารถนำเงินสดดิจิตอลที่ได้จากลูกค้าไปใช้ต่อได้

4. การทอนเงิน

- กรณีราคาสินค้า หรือบริการ น้อยกว่าจำนวนเงินสดดิจิตอล ร้านค้าจะทอนเงินสดให้ลูกค้าแทนเงินสดดิจิตอล เนื่องจากลูกค้าไม่สามารถตรวจสอบความถูกต้องของเงินทอนจากร้านค้าได้

5. การตรวจพบการทุจริต

- บุคคลที่ถูกตรวจพบการทุจริตเป็นครั้งแรกจะถูกบันทึกลงฐานข้อมูลผู้ทุจริต โดยมีสถานะเป็นผู้ต้องสงสัย

- บุคคลที่ถูกตรวจพบการทุจริตเป็นครั้งที่สอง โดยข้อมูลการทุจริตครั้งแรกอยู่ในสถานะผู้ต้องสงสัย บุคคลดังกล่าวจะยังสามารถดำเนินการซื้อเงินสดดิจิตอลได้

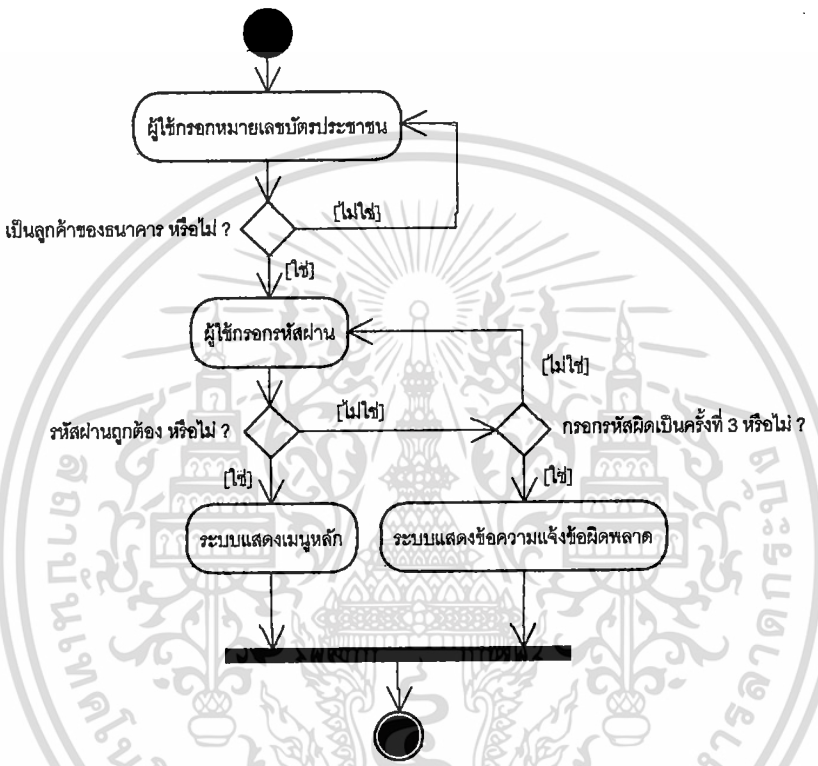
- บุคคลที่ถูกตรวจพบการทุจริตเป็นครั้งที่สอง โดยข้อมูลการทุจริตครั้งแรกอยู่ในสถานะผู้กระทำผิด บุคคลดังกล่าวจะไม่สามารถดำเนินการซื้อเงินสดดิจิตอลได้ ต้องติดต่อกับธนาคาร เพื่อดำเนินการชดใช้ทางกฎหมายให้เรียบร้อยก่อน จึงจะสามารถแก้ไข หรือลบข้อมูลผู้ทุจริตนั้นออกจากฐานข้อมูลการทุจริตได้

3.3 แผนภาพกิจกรรม (Activity Diagram)

ในส่วนนี้เป็นการอธิบายกิจกรรมการทำงานของแต่ละยูสเคสที่ออกแบบไว้ในตอนแรก แสดงให้เห็นถึงรายละเอียดกิจกรรมที่เกิดขึ้นในแต่ละส่วนของระบบ

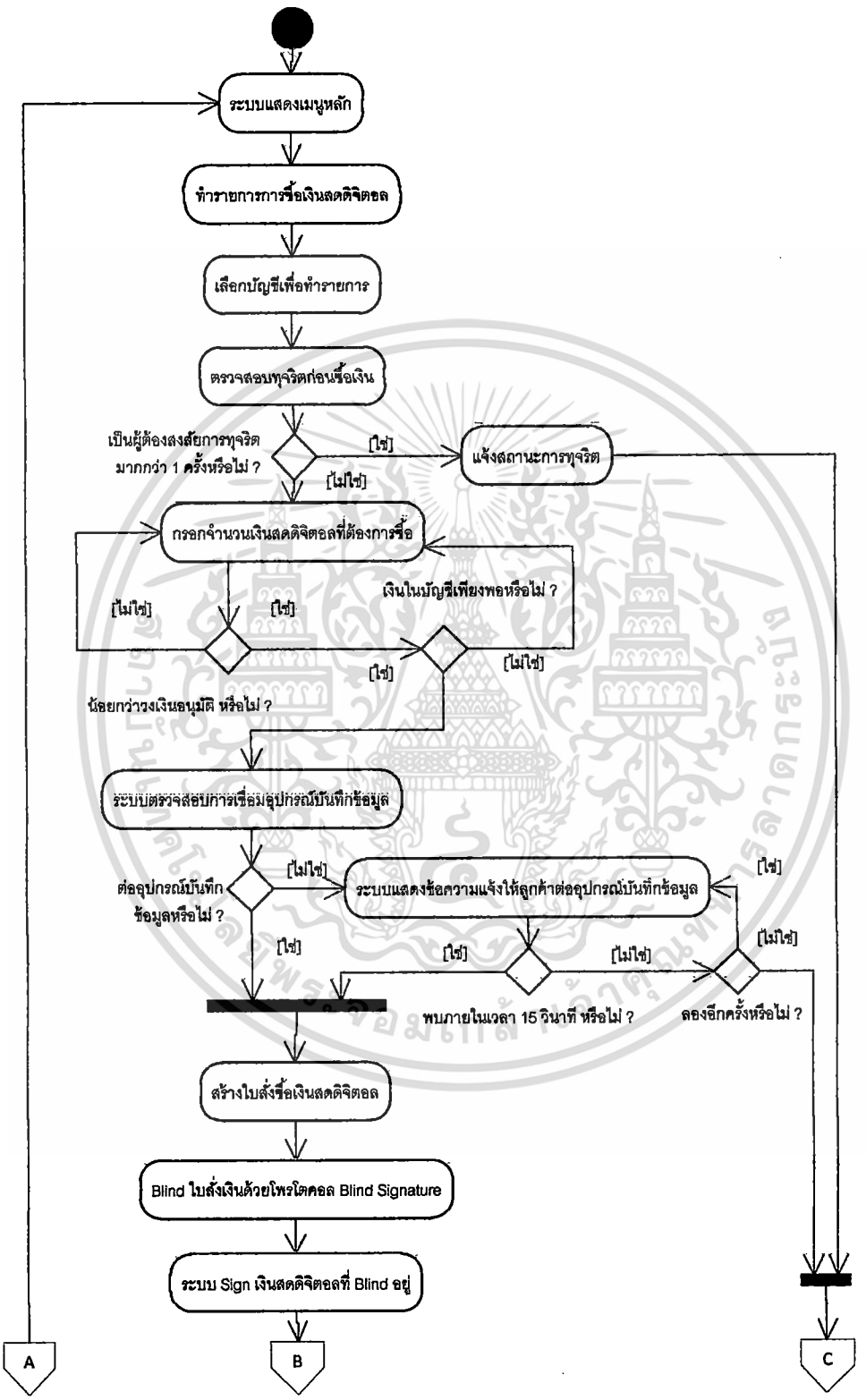
3.3.1 แผนภาพกิจกรรมของยูสเคสในระบบแลกเปลี่ยนเงินสดดิจิตอล

1. แผนภาพกิจกรรมของยูสเคส Login ของระบบแลกเปลี่ยนเงินสดดิจิตอล ดังรูปที่ 3.2

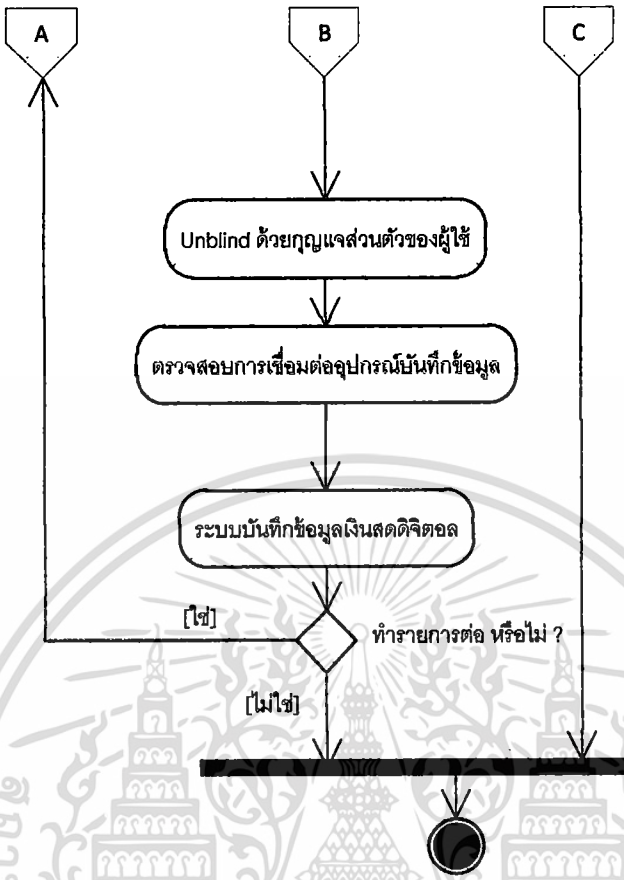


รูปที่ 3.2 แผนภาพกิจกรรมของยูสเคส Login ของระบบแลกเปลี่ยนเงินสดดิจิตอล

2. แผนภาพกิจกรรมของยูสเคส Purchase Digital Cash ของระบบแลกเปลี่ยนเงินสดดิจิตอล ดังรูปที่ 3.3 และรูปที่ 3.4

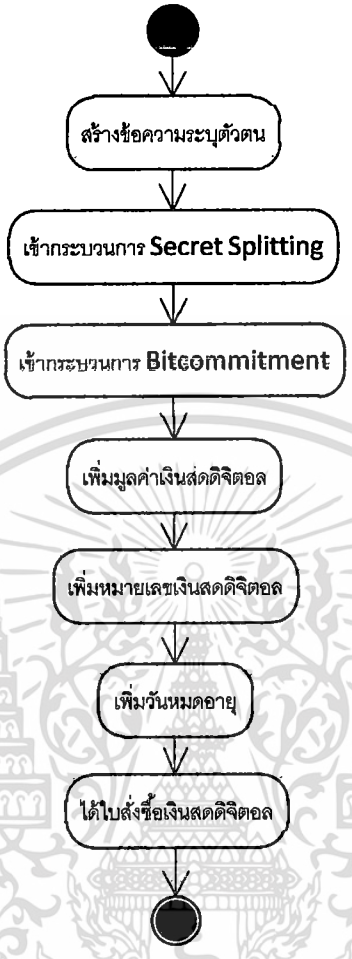


รูปที่ 3.3 แผนภาพกิจกรรมของยูสเคส Purchase Digital Cash ของระบบแลกเปลี่ยนเงินสดดิจิตอล



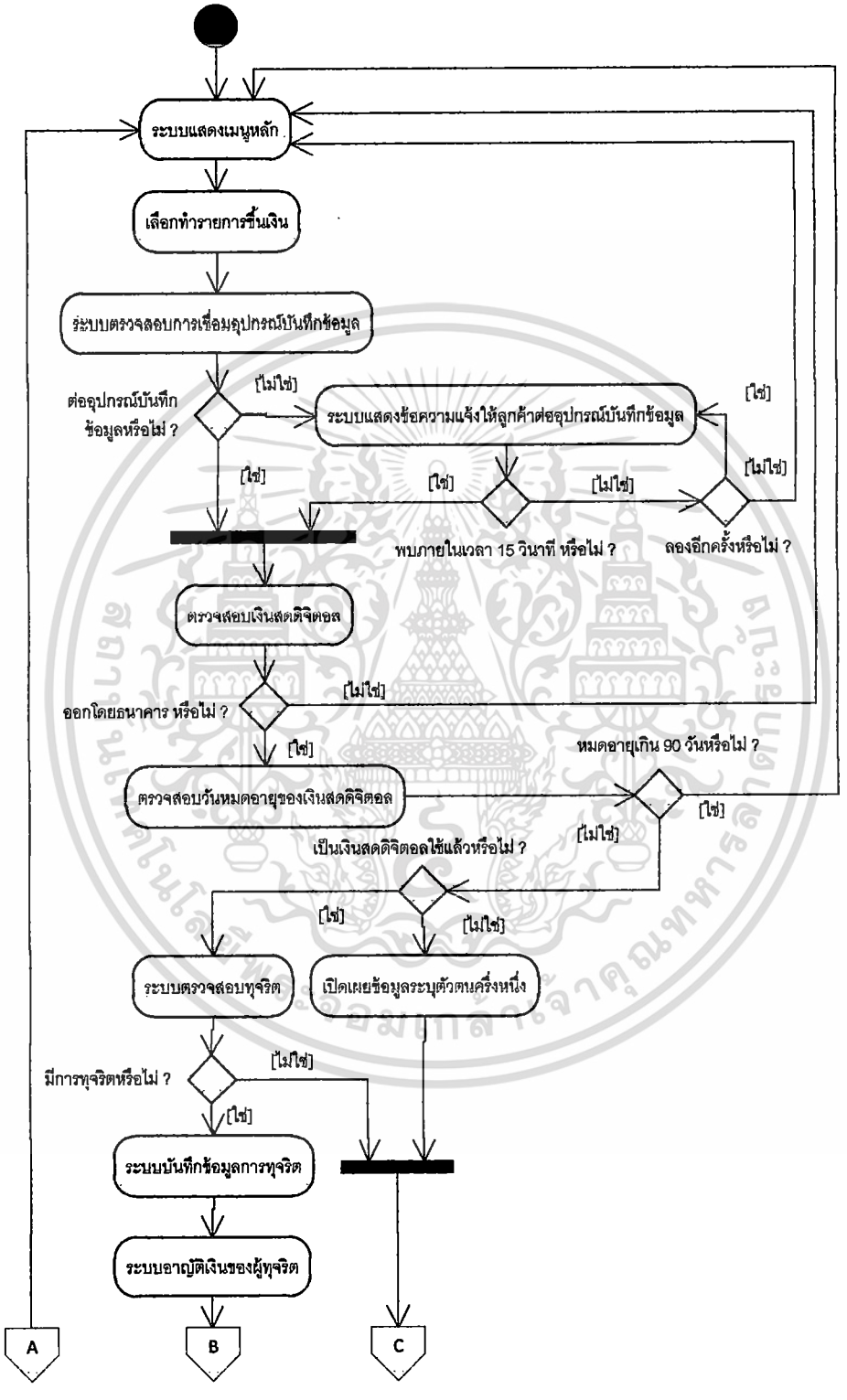
รูปที่ 3.4 (ต่อ) แผนภาพกิจกรรมของยูสเคส Purchase Digital Cash ของระบบแลกเปลี่ยนเงินสดดิจิตอล

แผนภาพกิจกรรมการสร้างใบสั่งซื้อเงินสดดิจิตอลในยูสเคส Purchase Digital Cash ของระบบแลกเปลี่ยนเงินสดดิจิตอล ดังรูปที่ 3.5

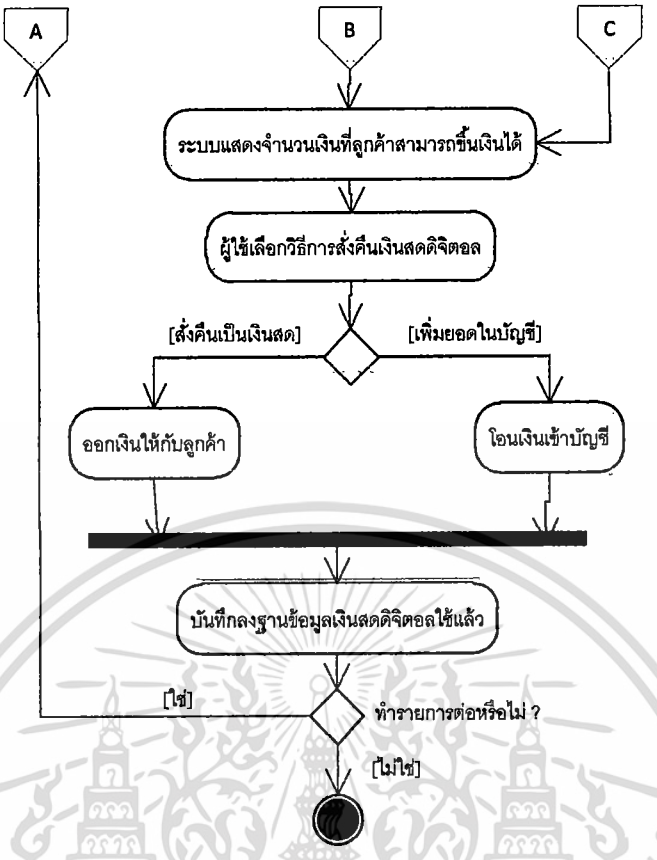


รูปที่ 3.5 แผนภาพกิจกรรมการสร้างใบสั่งเงินสดดิจิตอลในยูสเคส Purchase Digital Cash ของระบบแลกเปลี่ยนเงินสดดิจิตอล

3. แผนภาพกิจกรรมของยูสเยสคืนเงิน หรือขึ้นเงิน ของระบบแลกเปลี่ยนเงินสดดิจิตอล ดังรูปที่ 3.6 และรูปที่ 3.7

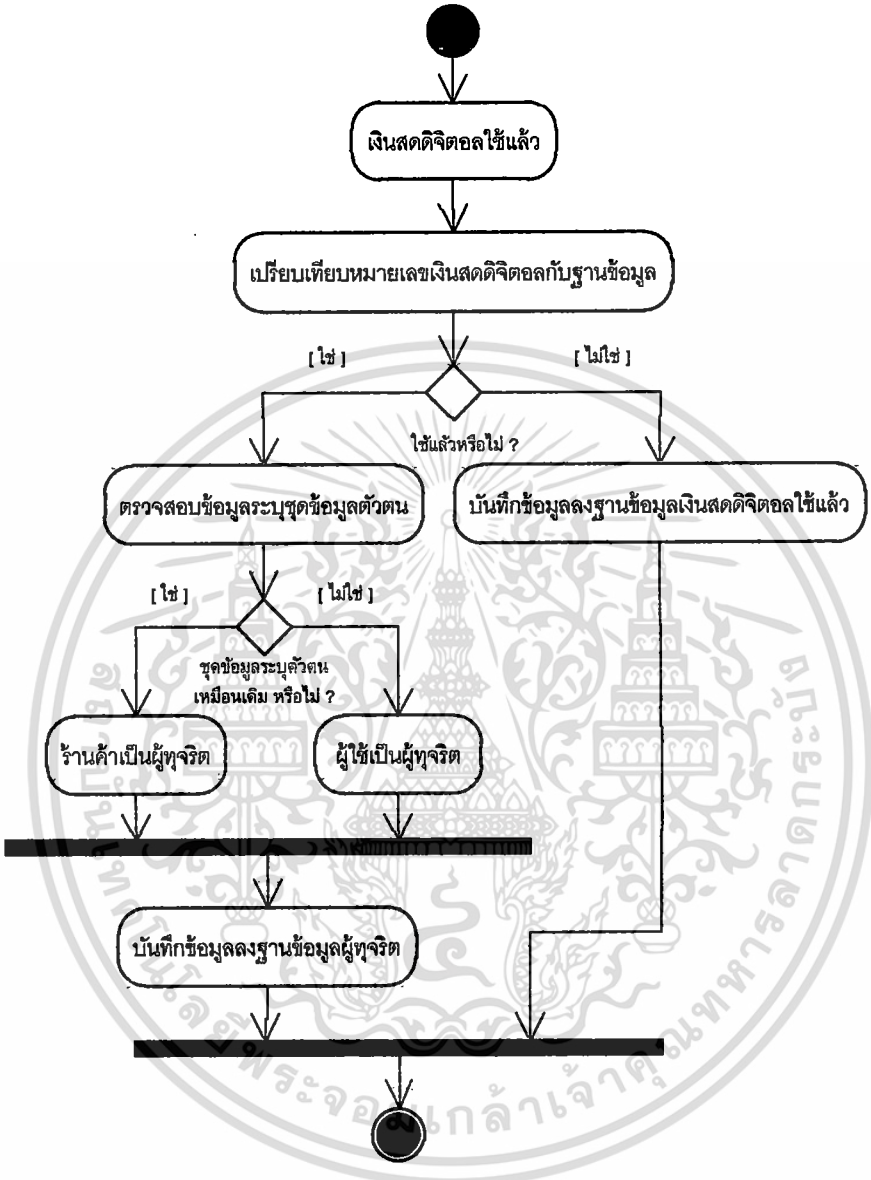


รูปที่ 3.6 แสดงแผนภาพกิจกรรมของยูสเคสคืนเงิน หรือขึ้นเงินของระบบแลกเปลี่ยนเงินสดดิจิตอล



รูปที่ 3.7 (ต่อ) แสดงแผนภาพกิจกรรมของยูสเคสคืนเงิน หรือขึ้นเงินของระบบแลกเปลี่ยนเงินสดดิจิตอล

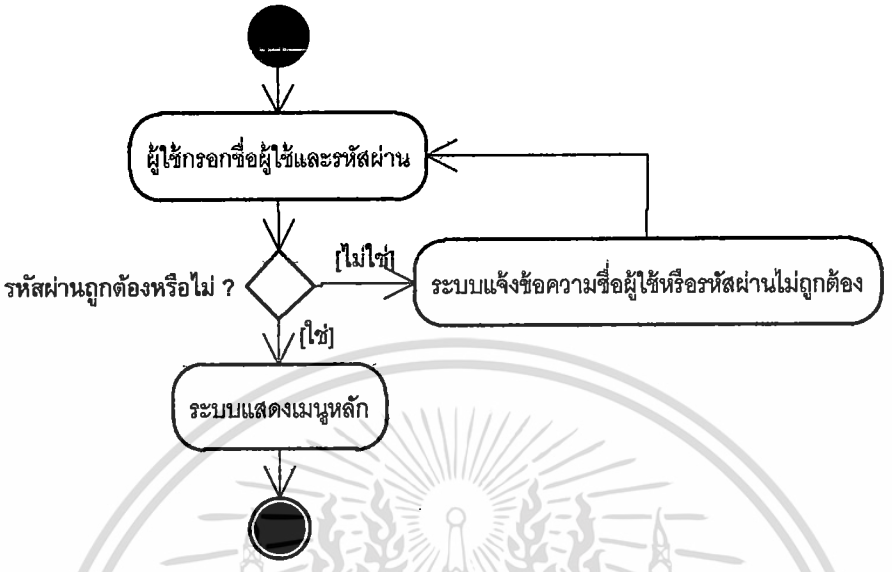
4. แผนภาพแสดงกิจกรรมของยูสเคสการตรวจสอบทุจริตของระบบแลกเปลี่ยนเงินสดดิจิตอล ดังรูปที่ 3.8



รูปที่ 3.8 แผนภาพกิจกรรมของยูสเคสการตรวจสอบทุจริตของระบบแลกเปลี่ยนเงินสดดิจิตอล

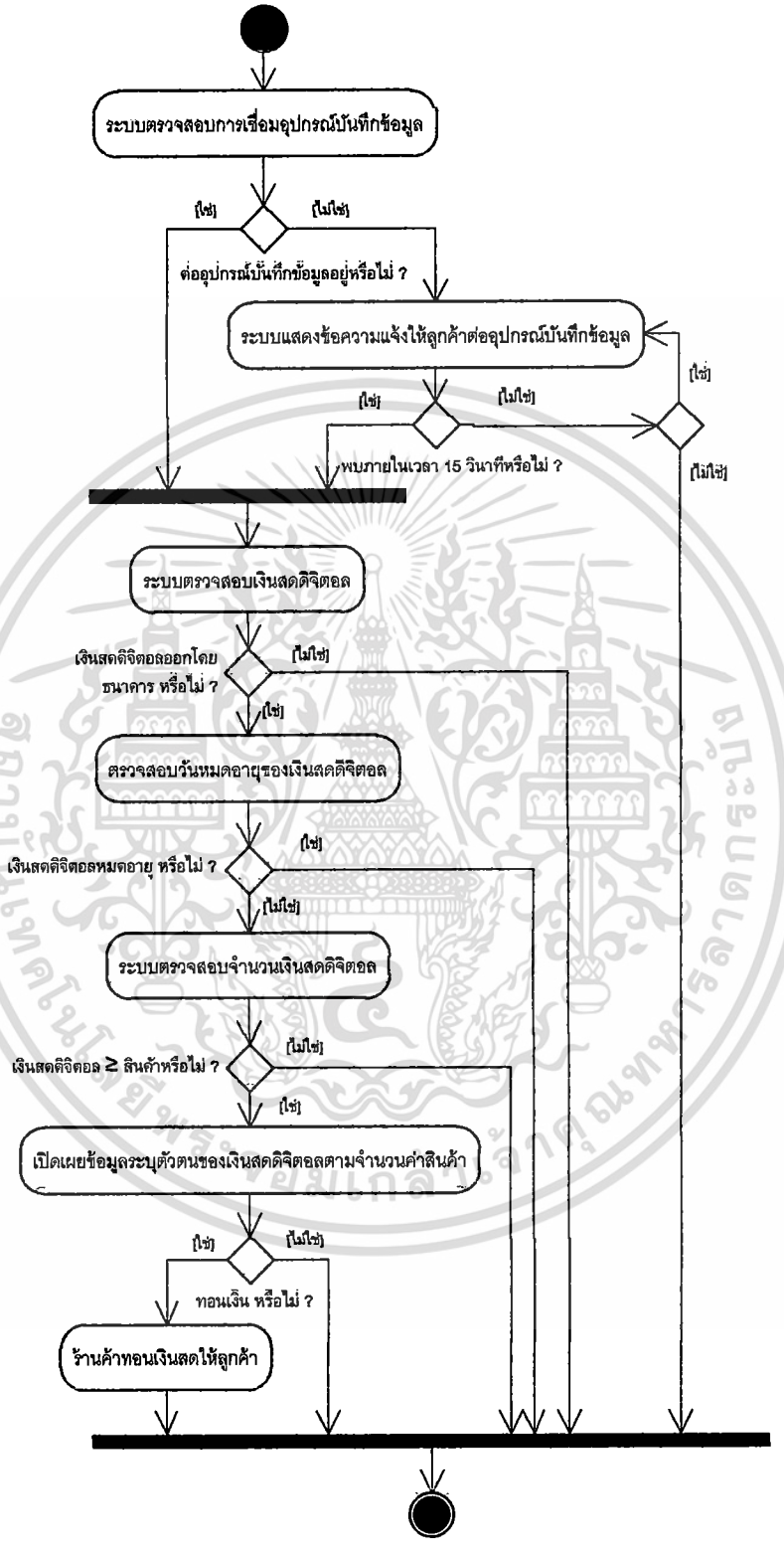
3.3.2 แผนภาพกิจกรรมยูสเคสของระบบเงินสดดิจิตอลสำหรับร้านค้า

1. แผนภาพกิจกรรมของยูสเคส Login ของระบบฯสำหรับร้านค้า ดังรูปที่ 3.9



รูปที่ 3.9 แผนภาพกิจกรรมของยูสเคส Login ของระบบฯสำหรับร้านค้า

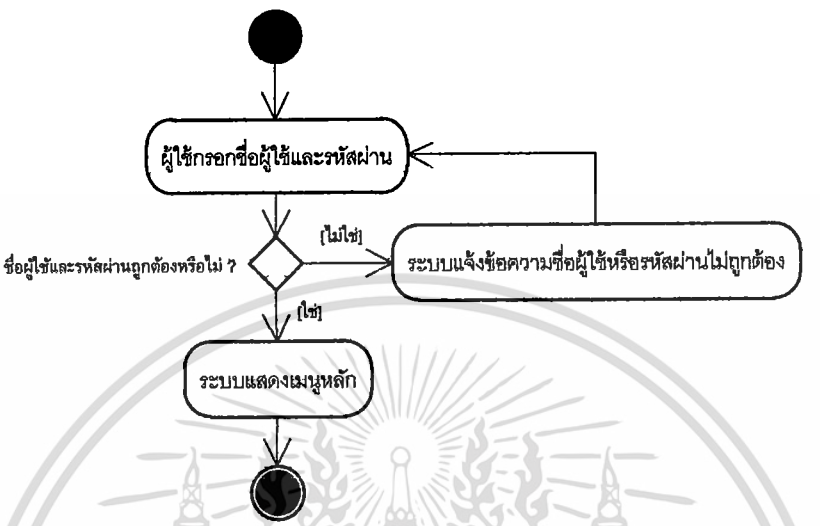
2. แผนภาพกิจกรรมของยูสเคสซื้อ-ขายของระบบฯสำหรับร้านค้า ดังรูปที่ 3.10



รูปที่ 3.10 แสดงแผนภาพกิจกรรมของยูสเคสซื้อ-ขายของระบบฯสำหรับร้านค้า

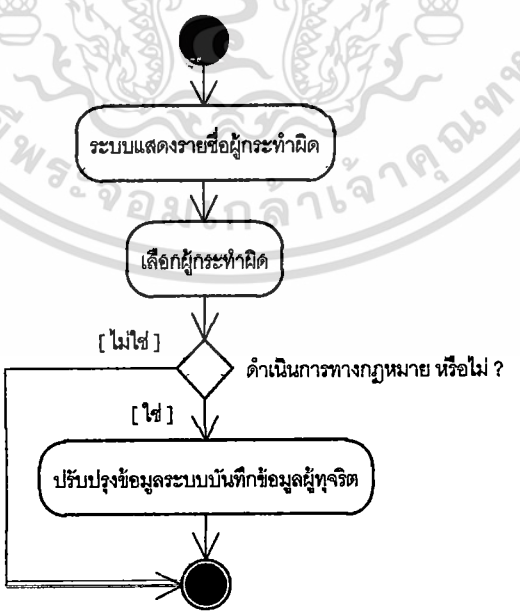
3.3.3 แผนภาพกิจกรรมยูสเคสของระบบเงินสดดิจิตอลสำหรับผู้ดูแลระบบ

1. แผนภาพกิจกรรมยูสเคส Login ของระบบเงินสดดิจิตอลสำหรับผู้ดูแลระบบ ดังรูปที่ 3.11



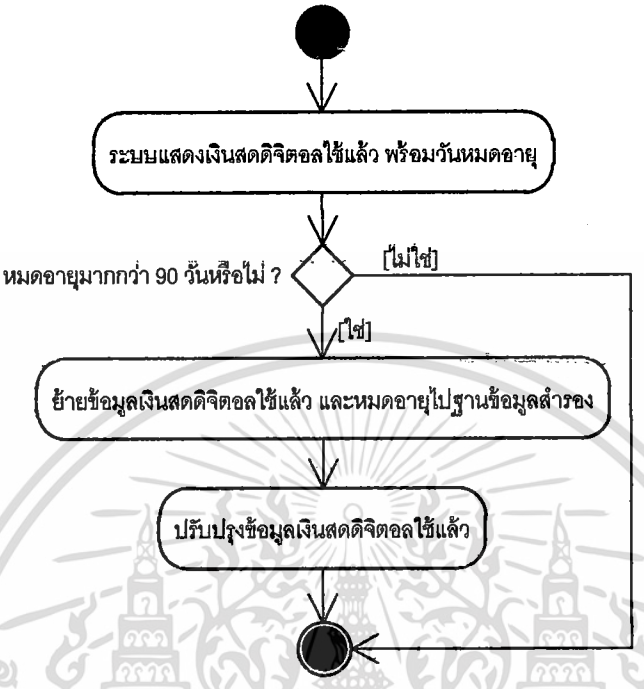
รูปที่ 3.11 แสดงแผนภาพกิจกรรมยูสเคส Login ของระบบสำหรับผู้ดูแลระบบ

2. แผนภาพกิจกรรมยูสเคสการจัดการผู้กระทำผิดของระบบเงินสดดิจิตอลสำหรับผู้ดูระบบ ดังรูปที่ 3.12



รูปที่ 3.12 แสดงแผนภาพกิจกรรมยูสเคสการจัดการผู้กระทำผิดของระบบฯสำหรับผู้ดูแลระบบ

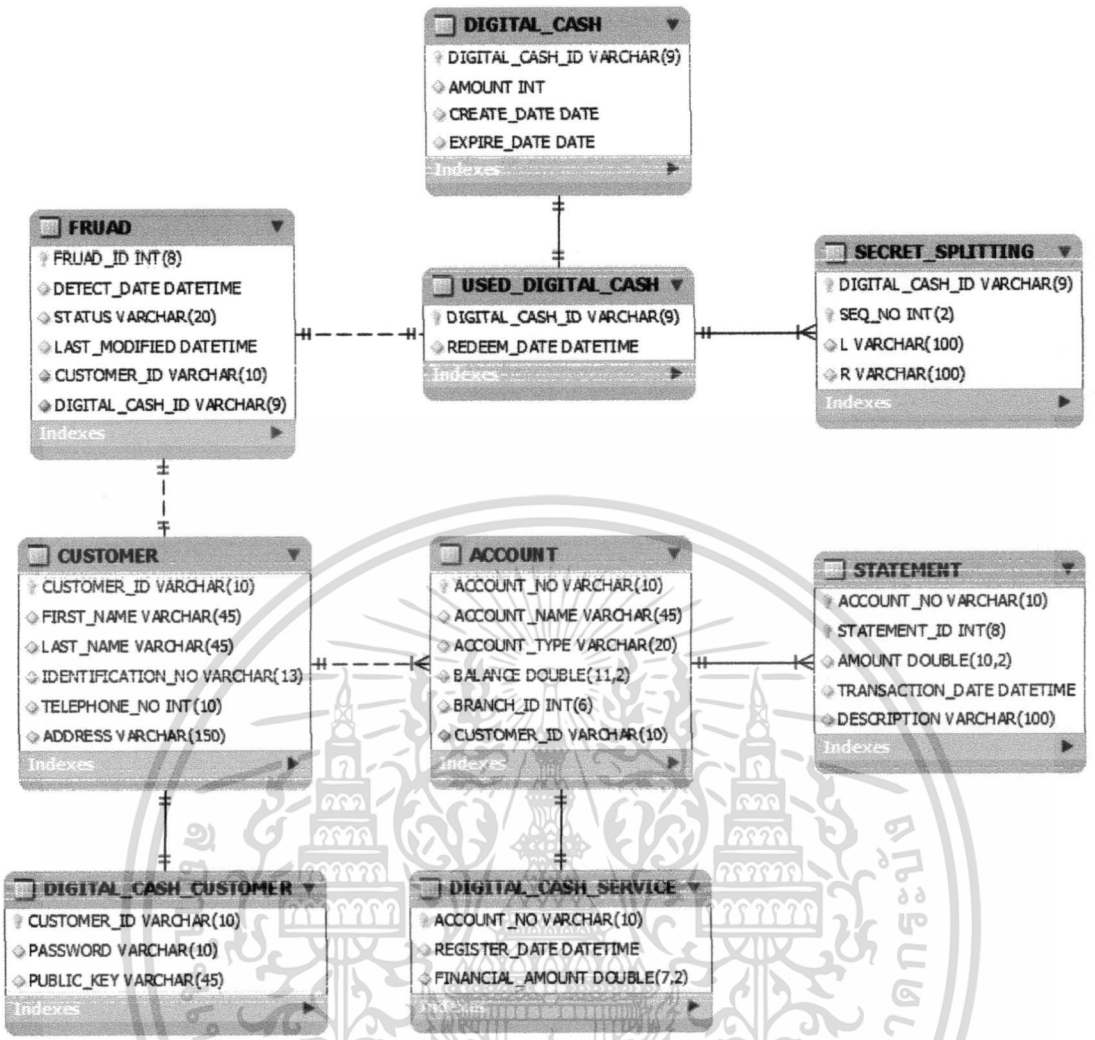
3. แผนภาพกิจกรรมยูสเคสการจัดการเงินสดดิจิตอลใช้แล้วของระบบเงินสดดิจิตอลสำหรับผู้ดูแลระบบ ดังรูปที่ 3.13



รูปที่ 3.13 แสดงแผนภาพกิจกรรมยูสเคสการจัดการเงินสดดิจิตอลใช้แล้วของระบบฯสำหรับผู้ดูแลระบบ

3.4 ระบบฐานข้อมูล

ฐานข้อมูลจะอยู่ที่ฝั่งของธนาคาร ซึ่งทั้งระบบแลกเปลี่ยนเงินสดดิจิตอล และระบบเงินสดดิจิตอลสำหรับผู้ดูแลระบบจำเป็นต้องเชื่อมต่อกับฐานข้อมูลนี้สำหรับดึงข้อมูลเพื่อแสดงผล และดำเนินการต่างๆ โดยการพัฒนาระบบเงินสดดิจิตอลนี้ใช้ฐานข้อมูลของ MySQL ที่มีรูปแบบความสัมพันธ์ของตารางข้อมูล 9 ตารางตามที่ได้แสดงในรูปที่ 3.14



รูปที่ 3.14 แผนภาพความสัมพันธ์ระหว่างตารางในฐานข้อมูล

บทที่ 4
ต้นแบบระบบเงินสดดิจิตอลชนิดออฟไลน์ที่พัฒนาขึ้น

4.1 ส่วนประกอบของระบบ

4.1.1 ผู้ใช้งานระบบ

1. ผู้ใช้ที่ซื้อเงินสดดิจิตอล เกี่ยวข้องกับระบบแลกเปลี่ยนเงินสดดิจิตอล ผู้ใช้ที่ซื้อเงินสดดิจิตอลได้ ต้องมีคุณสมบัติที่สำคัญ 2 ประการ คือ บุคคลผู้นั้นต้องมีบัญชีกับธนาคาร และบัญชีดังกล่าวต้องสมัครใช้บริการเงินสดดิจิตอลกับธนาคาร จึงจะสามารถดำเนินการซื้อเงินสดดิจิตอลจากธนาคารได้

2. ผู้ใช้ที่นำเงินสดดิจิตอลมาขึ้นเงิน เกี่ยวข้องกับระบบแลกเปลี่ยนเงินสดดิจิตอล ผู้ใช้ที่สามารถนำเงินสดดิจิตอลมาขึ้นเงินกับธนาคารได้ ต้องมีคุณสมบัติที่สำคัญ 2 ประการ เช่นเดียวกับการซื้อเงิน คือ ต้องมีบัญชีกับธนาคาร และต้องสมัครใช้บริการเงินสดดิจิตอลกับธนาคารด้วย โดยผู้ที่นำเงินสดดิจิตอลมาคืนเงิน หรือขึ้นเงินอาจเป็นได้ทั้งผู้ซื้อ และผู้ขาย ส่วนการขึ้นเงินจะสามารถทำได้อย่างสมบูรณ์ก็ต่อเมื่อ ผู้ที่นำเงินมาคืนเงิน หรือขึ้นเงินนั้นต้องไม่เป็นผู้ทุจริต จึงจะสามารถคืนเงิน หรือขึ้นเงินสดดิจิตอลได้

3. ร้านค้า เกี่ยวข้องกับระบบเงินสดดิจิตอลสำหรับร้านค้า ร้านค้าสามารถตรวจสอบเงินสดดิจิตอลที่นำมาใช้ชำระสินค้า หรือบริการได้ว่า เป็นเงินสดที่ออกโดยธนาคารอย่างถูกต้องหรือไม่ หากไม่ถูกต้องขั้นตอนการซื้อขายจะไม่เกิดขึ้น

4. เจ้าหน้าที่ธนาคาร เกี่ยวข้องกับระบบเงินสดดิจิตอลสำหรับผู้ดูแลระบบ เจ้าหน้าที่ธนาคารทำหน้าที่เฝ้าระวัง คอยจัดการกับข้อมูลเงินสดดิจิตอลใช้แล้ว และดำเนินการเอาผิดกับรายชื่อผู้ทุจริตในฐานข้อมูล

4.1.2 กุญแจ (Keys)

กุญแจในระบบประกอบด้วย 2 ส่วน คือ กุญแจสาธารณะ(Public Key) และกุญแจส่วนตัว (Private Key) กุญแจทั้งคู่จะถูกสร้างขึ้นพร้อมกันแต่จัดเก็บแยกกัน คือ ธนาคารจะเก็บกุญแจสาธารณะของผู้ใช้ไว้ ส่วนกุญแจส่วนตัวของผู้ใช้ จะถูกบันทึกลงในอุปกรณ์บันทึกข้อมูลพร้อมกับข้อมูลเงินสดดิจิตอล

4.1.3 เงินสดดิจิตอล

1. เงินสดดิจิตอลยังไม่ถูกใช้ เงินสดดิจิตอลที่ยังไม่ได้ใช้ ได้จากระบบแลกเปลี่ยนเงินสดดิจิตอล เงินดังกล่าวนี้ได้ถูกออกโดยธนาคาร หรือเข้ารหัสลับโดยธนาคารอย่างถูกต้องเรียบร้อย สามารถนำเงินสดดิจิตอลที่ยังไม่ถูกใช้นี้ในการชำระค่าสินค้า หรือบริการได้ นอกจากนั้นเงินสดดิจิตอลที่ยังไม่ถูกใช้จะต้องยังไม่ถูกเปิดเผยข้อมูลระบุตัวตนเช่นกัน

2. เงินสดดิจิตอลใช้แล้ว เงินสดดิจิตอลที่ยังไม่ถูกใช้จะถูกเปลี่ยนสถานะเป็นเงินสดดิจิตอลใช้แล้วที่ระบบเงินสดดิจิตอลสำหรับร้านค้า คือ หลังจากใช้เงินสดดิจิตอลนั้นในการชำระสินค้า หรือบริการ เงินสดดิจิตอลจะถูกเปิดข้อมูลระบุตัวตนครั้งหนึ่ง ทำให้เงินสดดิจิตอลที่ยังไม่ถูกใช้ เปลี่ยนสถานะเป็นเงินสดดิจิตอลใช้แล้ว

4.1.4 อุปกรณ์บันทึกข้อมูล

อุปกรณ์บันทึกข้อมูลทำหน้าที่บันทึกกุญแจส่วนตัวของผู้ใช้ (Private Key) และไฟล์เงินสดดิจิตอลที่ได้จากระบบแลกเปลี่ยนเงินสดดิจิตอล เพื่อนำไปใช้ในการชำระสินค้า หรือบริการที่ร้านค้าที่มีระบบเงินสดดิจิตอลสำหรับร้านค้าอยู่

4.1.5 ฐานข้อมูล

ฐานข้อมูลจะอยู่ที่ฝั่งของธนาคารทั้งระบบแลกเปลี่ยนเงินสดดิจิตอล และระบบเงินสดดิจิตอลสำหรับผู้ดูแลระบบต้องมีการเชื่อมต่อกับฐานข้อมูลนี้อยู่ตลอดเวลา ฐานข้อมูลจะทำหน้าที่เก็บข้อมูลของลูกค้า, บัญชีของลูกค้า, ข้อมูลผู้ทุจริต และข้อมูลเงินสดดิจิตอลใช้แล้ว โดยระบบทั้ง 2 จะนำข้อมูลเหล่านี้จากฐานข้อมูล เพื่อใช้ในการทำงานของระบบ

4.1.6 ซอฟต์แวร์ระบบ

ซอฟต์แวร์ที่ใช้ในระบบเงินสดดิจิตอลชนิดออฟไลน์นี้ถูกพัฒนาขึ้นด้วยภาษา JAVA บนเครื่องคอมพิวเตอร์ที่ติดตั้งระบบปฏิบัติการไมโครซอฟต์วินโดว์เซเว่น (Microsoft Windows7) ประกอบด้วยระบบย่อย 3 ระบบคือ

1. ระบบแลกเปลี่ยนเงินสดดิจิตอล
2. ระบบเงินสดดิจิตอลสำหรับร้านค้า
3. ระบบเงินสดดิจิตอลสำหรับผู้ดูแลระบบ

4.2 การทำงานของระบบ

4.2.1 ขั้นตอนการซื้อเงิน

1. ผู้ใช้กรอกหมายเลขบัตรประจำตัวประชาชน และรหัสผ่าน เพื่อขอเข้าใช้งานระบบ

2. ผู้ใช้เลือกทำรายการการซื้อเงิน
3. ระบบแสดงรายการบัญชีทั้งหมดของผู้ใช้ที่สมัครบริการเงินสดดิจิตอลแล้ว
4. ผู้ใช้เลือกบัญชีที่ต้องการทำรายการ
5. ระบบแสดงข้อความร้องขอการเชื่อมต่ออุปกรณ์บันทึกข้อมูล
6. ผู้ใช้เชื่อมต่ออุปกรณ์บันทึกข้อมูล
7. ระบบแสดงจำนวนเงินที่ลูกค้าสามารถซื้อได้
8. ลูกค้ากรอกจำนวนเงินสดดิจิตอลที่ต้องการซื้อ
9. ระบบสร้างใบสั่งเงิน จากนั้นเข้าสู่กระบวนการ Blind Signature
10. ระบบแสดงผลการทำงานแก่ผู้ใช้
11. ลูกค้ายืนยันการซื้อเงินสดดิจิตอล
12. ระบบบันทึกข้อมูลเงินสดดิจิตอลลงอุปกรณ์บันทึกข้อมูล พร้อมแสดงข้อความเสร็จการดำเนินการ

4.2.2 ขั้นตอนการสร้างใบสั่งเงิน

1. ใช้หมายเลขบัญชี และหมายเลขบัตรประจำตัวประชาชนสำหรับการสร้างข้อความระบุตัวตน
2. ใช้โพรโตคอล Secret Splitting แยกข้อความออกเป็นส่วนๆ เพื่อรักษาความเป็นส่วนตัวให้กับผู้ใช้ และใช้เพื่อตรวจสอบทุจริตหากมีการทุจริตเกิดขึ้น
3. นำแต่ละส่วนของข้อมูลที่ได้จาก Secret Splitting เข้ากระบวนการ Bit- Commitment เพื่อป้องกันการเปลี่ยนแปลงข้อมูลของผู้ใช้
4. ระบบนำชุดข้อมูลที่ได้รวมกับเฮดเดอร์มูลค่าเงิน หมายเลขเงินสดดิจิตอล และวันหมดอายุ
5. ได้เป็นข้อมูลใบสั่งเงินสดดิจิตอล เพื่อทำการ Blind Signature ต่อไป

4.2.3 ขั้นตอนการคืนเงิน หรือขึ้นเงิน

1. ผู้ใช้กรอกหมายเลขบัตรประจำตัวประชาชน และรหัสผ่าน เพื่อขอเข้าใช้งานระบบ
2. ผู้ใช้เลือกทำรายการการขึ้นเงินสดดิจิตอล
3. ระบบตรวจสอบความถูกต้องของเงินสดดิจิตอลดังกล่าว ว่าถูกออกโดยธนาคารหรือไม่
4. ระบบตรวจสอบวันหมดอายุของเงินสดดิจิตอล ว่าหมดอายุหรือไม่
5. ระบบตรวจสอบทุจริตของเงินสดดิจิตอล

6. ระบบแสดงจำนวนเงินสดดิจิตอลที่สามารถขึ้นเงินได้ พร้อมทางเลือกในการขึ้นเงินสดดิจิตอล คือ เงินสด และโอนเข้าบัญชี

7. ผู้ใช้เลือกวิธีการขึ้นเงิน

8. ระบบจ่ายเงินตามวิธีที่ลูกค้าเลือก

9. ระบบบันทึกข้อมูลเงินสดดิจิตอลใช้แล้วลงฐานข้อมูลเงินสดดิจิตอลใช้แล้ว

4.2.4 ขั้นตอนการซื้อสินค้า และทอนเงิน

1. ลูกค้าจ่ายเงินสดดิจิตอล เพื่อชำระค่าสินค้า หรือบริการให้ร้านค้า

2. ระบบตรวจสอบความถูกต้องของเงินสดดิจิตอลว่าออกโดยธนาคาร หรือไม่

3. ระบบตรวจสอบวันหมดอายุของเงินสดดิจิตอล

4. ระบบตรวจสอบมูลค่าเงินว่าเพียงพอกับมูลค่าสินค้า หรือบริการที่ต้องชำระหรือไม่

5. หากมูลค่าของเงินสดดิจิตอลมากกว่ามูลค่าของสินค้า หรือบริการ ร้านค้าจะทำการทอนเงินสดกลับไปให้กับลูกค้า

4.2.5 ขั้นตอนการตรวจสอบทุจริต

1. ระบบรับเงินสดดิจิตอลที่ถูกเปิดเผยข้อมูลระบุตัวตนครั้งหนึ่งมาจากผู้ใช้

2. ระบบค้นหาหมายเลขเงินสดดิจิตอลที่เพิ่งได้รับมาจากผู้ใช้ในฐานข้อมูลเงินสดดิจิตอลใช้แล้ว หากตรวจพบหมายเลขเงินสดดิจิตอลในฐานข้อมูลเงินสดดิจิตอลใช้แล้ว แสดงว่าเงินสดดิจิตอลที่เพิ่งได้รับมามีการทุจริต ซึ่งเป็นไปได้ 2 กรณี คือ

- หากชุดข้อมูลระบุตัวตนของเงินสดดิจิตอลที่เพิ่งได้รับมาเหมือนกับชุดข้อมูลระบุตัวตนของเงินสดดิจิตอลในฐานข้อมูลเงินสดดิจิตอลใช้แล้ว แสดงว่าร้านค้า หรือผู้ที่นำเงินสดดิจิตอลนี้มาขึ้นเป็นผู้ทุจริต

- หากชุดข้อมูลระบุตัวตนของเงินสดดิจิตอลที่เพิ่งได้รับมาไม่ เหมือนกับชุดข้อมูลระบุตัวตนของเงินสดดิจิตอลในฐานข้อมูลเงินสดดิจิตอลใช้แล้ว แสดงว่าเจ้าของเงินสดดิจิตอลนี้เป็นผู้ทุจริต ซึ่งจะสามารถระบุตัวผู้กระทำผิดได้จากชุดข้อมูลระบุตัวตนที่ถูกเปิดเผยครบทั้งด้านซ้าย และด้านขวา

3. ระบบเพิ่มชื่อผู้ทุจริตลงในฐานข้อมูลผู้ทุจริตด้วยสถานะผู้ต้องสงสัย

4.2.6 ขั้นตอนการจัดการกับผู้ทุจริต

การจัดการกับผู้ทุจริตเป็นหน้าที่ของฝ่ายกฎหมายของธนาคาร โดยสถานะของผู้ทุจริตของระบบ ประกอบด้วย 3 สถานะ

1. **ผู้ต้องสงสัย** เป็นสถานะเริ่มต้นเมื่อตรวจพบการทุจริตในเงินสดดิจิตอล เพื่อเปิดโอกาสให้ผู้ทุจริตมีโอกาสพิสูจน์ความบริสุทธิ์ได้

2. **ผู้ทุจริต** เป็นสถานะที่หากผู้ทุจริตไม่สามารถหาหลักฐานเพื่อยืนยันความบริสุทธิ์ได้จะเข้าสู่กระบวนการชดใช้ทางกฎหมาย

3. **ชดใช้เรียบร้อย** เป็นสถานะที่ผู้ทุจริตดำเนินการชดใช้ตามกฎหมายเรียบร้อย

4.2.7 ขั้นตอนการจัดการกับเงินสดดิจิตอลใช้แล้ว

ข้อมูลเงินสดดิจิตอลใช้แล้วในฐานข้อมูลถูกจัดการโดยอัตโนมัติจากระบบ โดยระบบจะตรวจสอบวันหมดอายุของเงินสดดิจิตอล เงินสดดิจิตอลที่หมดอายุเกิน 90 วัน จะถูกย้ายเข้าสู่ระบบฐานข้อมูลสำรองของธนาคาร

4.3 ซอฟต์แวร์ระบบ

ระบบเงินสดดิจิตอลชนิดออฟไลน์นี้ ออกแบบหน้าต่างการใช้งานให้มีลักษณะคล้ายคลึงกับการใช้งานของตู้เอทีเอ็มทั่วไป เพื่อให้สะดวกต่อการใช้งานของผู้ใช้ และความเป็นไปได้ในการประยุกต์เข้ากับระบบจริงของธนาคาร โดยสิ่งที่ใช้สำหรับบันทึกข้อมูลเงินสดดิจิตอลของระบบนี้เรียกว่า “อุปกรณ์บันทึกข้อมูล” ซึ่งภาพรวมหน้าต่างการใช้งานของแต่ละส่วนมีดังนี้

4.3.1 ส่วนของระบบแลกเปลี่ยนเงินสดดิจิตอล

1. หน้าแรกของระบบ แสดงดังรูปที่ 4.1

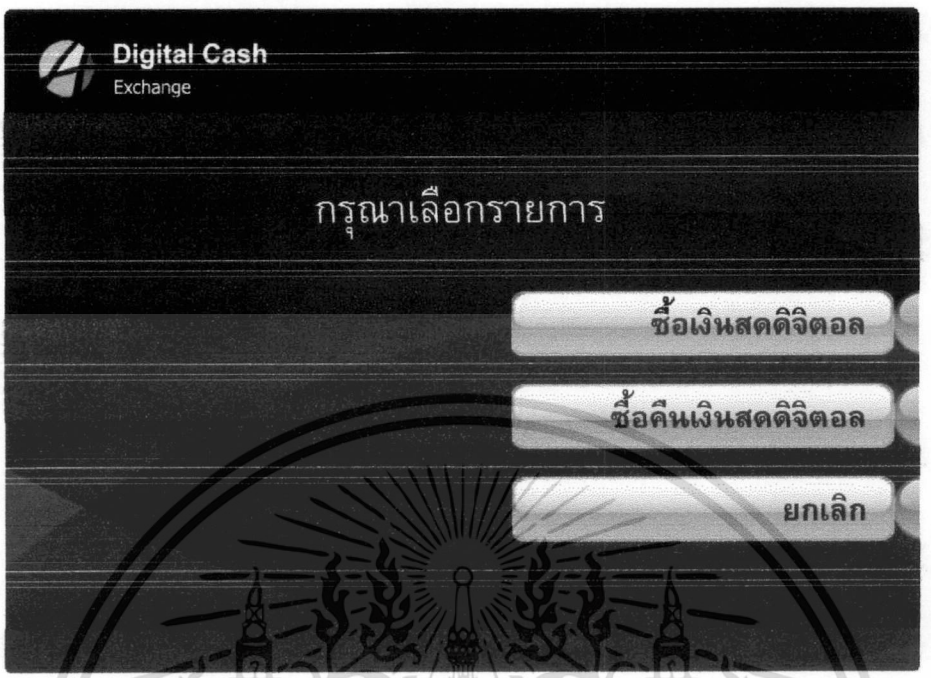
รูปที่ 4.1 หน้าแรกของระบบแลกเปลี่ยนเงินสดดิจิตอล

2. การเข้าใช้ระบบ แสดงดังรูปที่ 4.2 และรูปที่ 4.3

รูปที่ 4.2 หน้าต่างสำหรับกรอกหมายเลขบัตรประจำตัวประชาชนของผู้ใช้

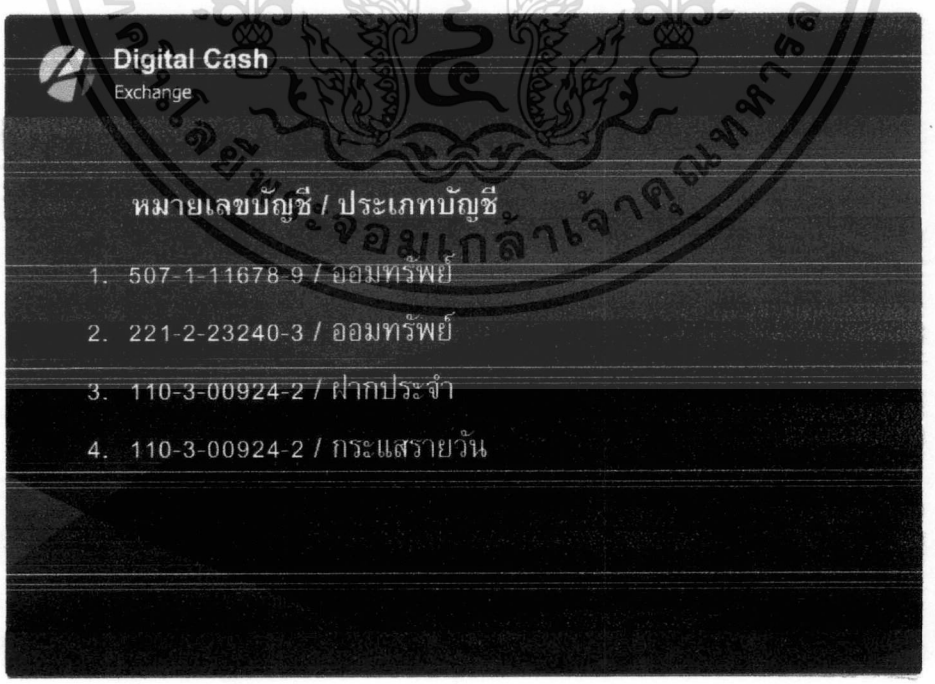
รูปที่ 4.3 หน้าต่างสำหรับกรอกรหัสผ่าน

3. ตัวเลือกการดำเนินการ แสดงดังรูปที่ 4.4

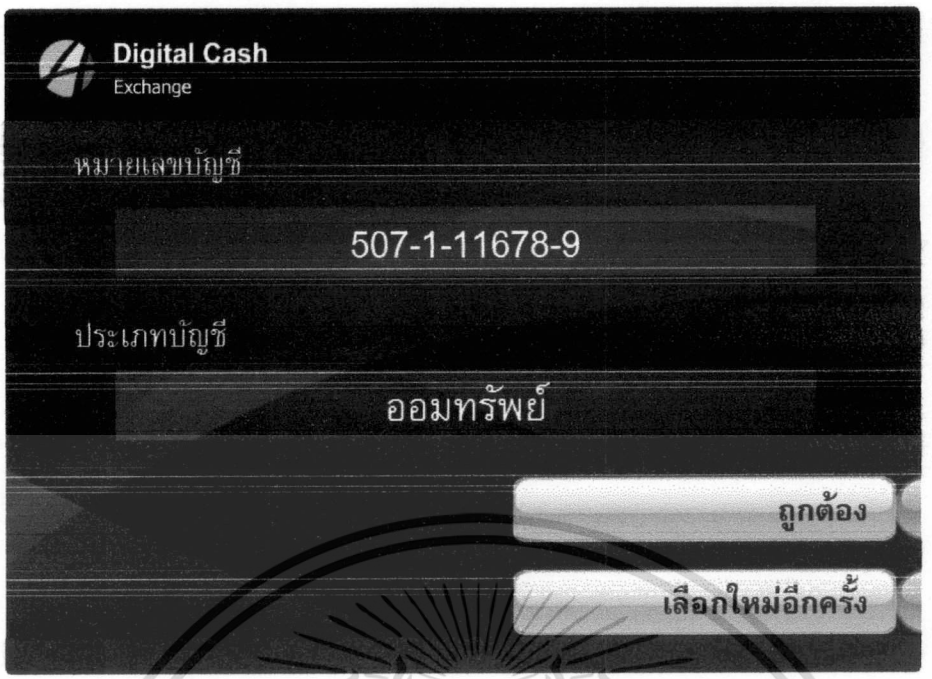


รูปที่ 4.4 แสดงรายการดำเนินการของระบบแลกเปลี่ยนเงินสดดิจิตอล

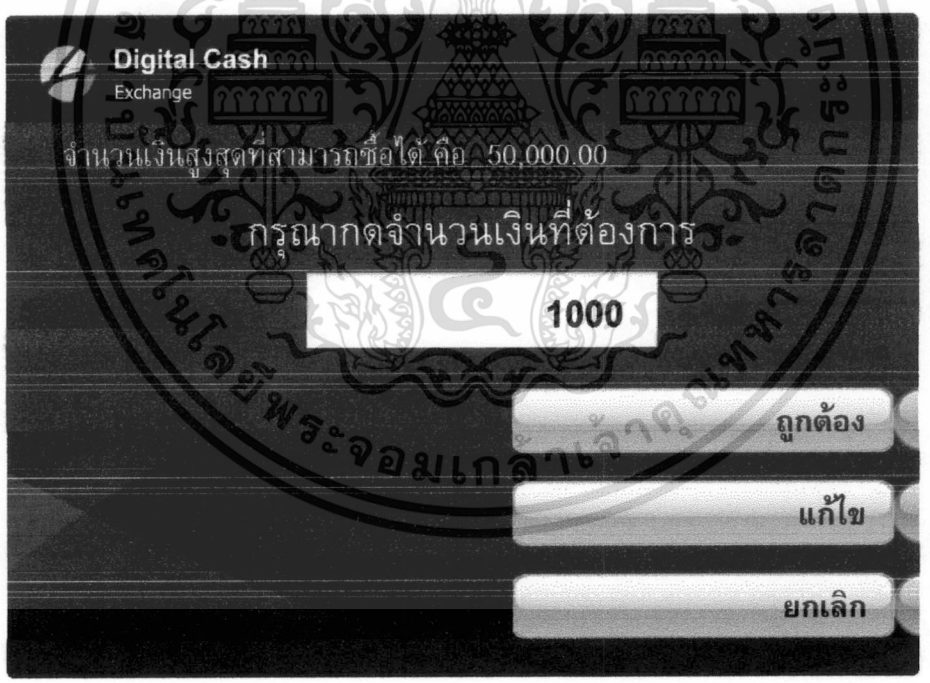
4. การซื้อเงิน แสดงดังรูปที่ 4.5 ถึงรูปที่ 4.11



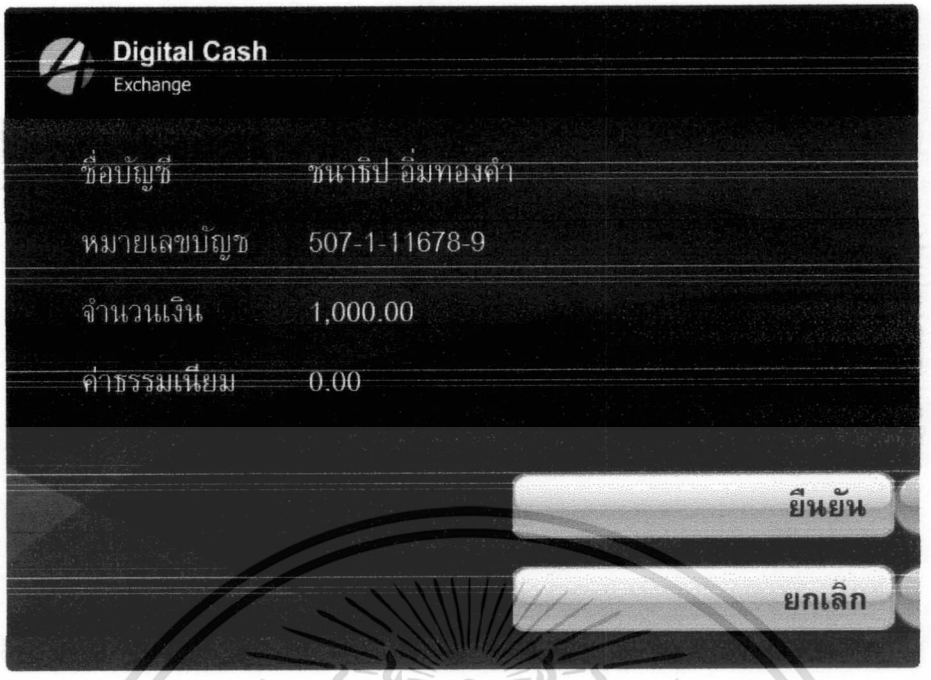
รูปที่ 4.5 แสดงรายชื่อบัญชีของผู้ใช้ที่สามารถซื้อเงินสดดิจิตอลได้



รูปที่ 4.6 แสดงบัญชีที่ผู้ใช้เลือก

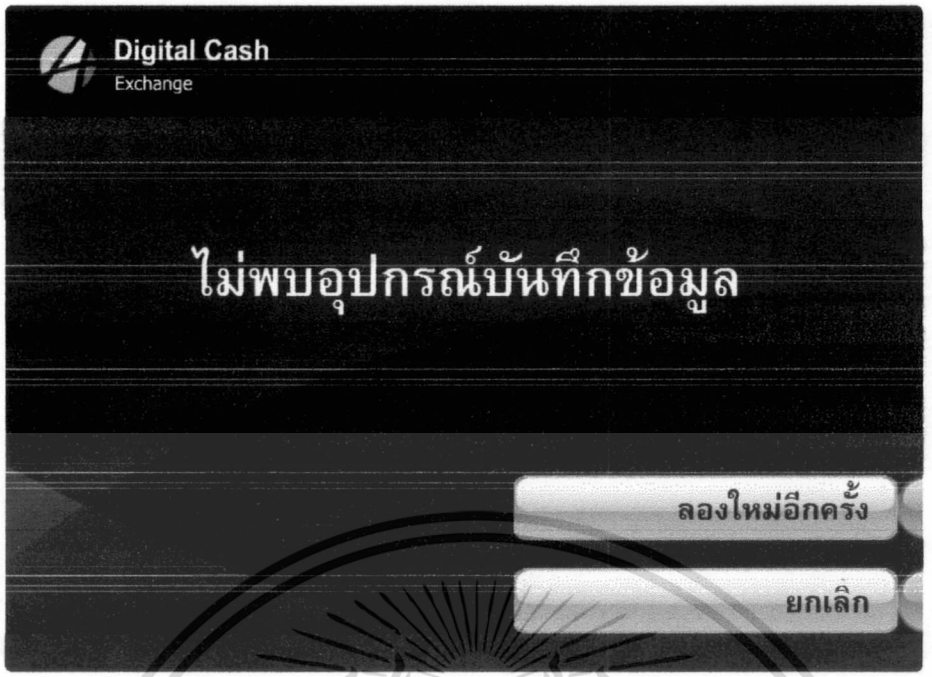


รูปที่ 4.7 หน้าต่างสำหรับกรอกจำนวนเงินสดดิจิตอลที่ต้องการซื้อ

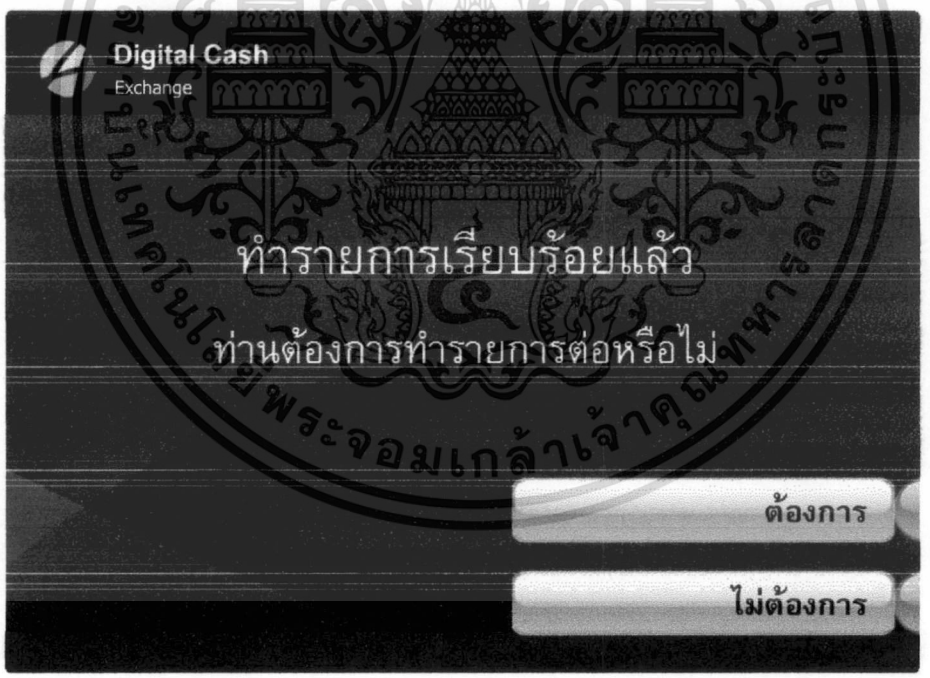


รูปที่ 4.8 แสดงรายละเอียดการซื้อเงินสดดิจิตอล

รูปที่ 4.9 ข้อความแจ้งเตือนผู้ใช้เพื่อเชื่อมต่ออุปกรณ์บันทึกข้อมูลเงินสดดิจิตอล



รูปที่ 4.10 ข้อความแจ้งเตือนไม่พบอุปกรณ์บันทึกข้อมูลเงินสดดิจิตอล

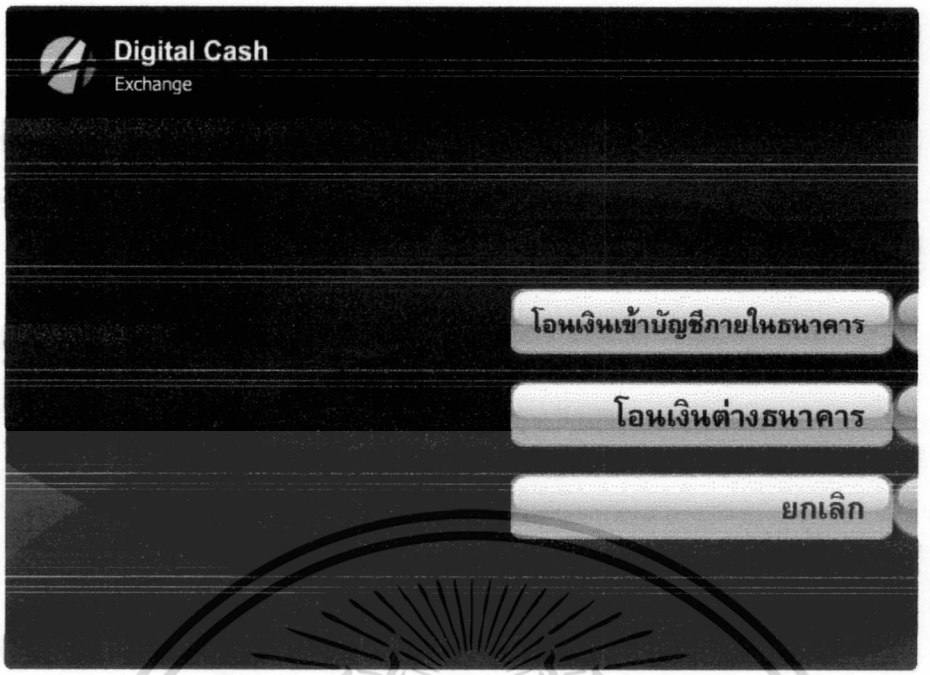


รูปที่ 4.11 ข้อความแสดงสถานะการดำเนินการซื้อเงินสดดิจิตอลเสร็จสิ้น

5. การคืนเงิน หรือขึ้นเงิน แสดงดังรูปที่ 4.12 ถึงรูปที่ 4.14

รูปที่ 4.12 แสดงจำนวนเงินสดดิจิตอลที่สามารถขึ้นเงินได้

รูปที่ 4.13 แสดงตัวเลือกการขึ้นเงิน



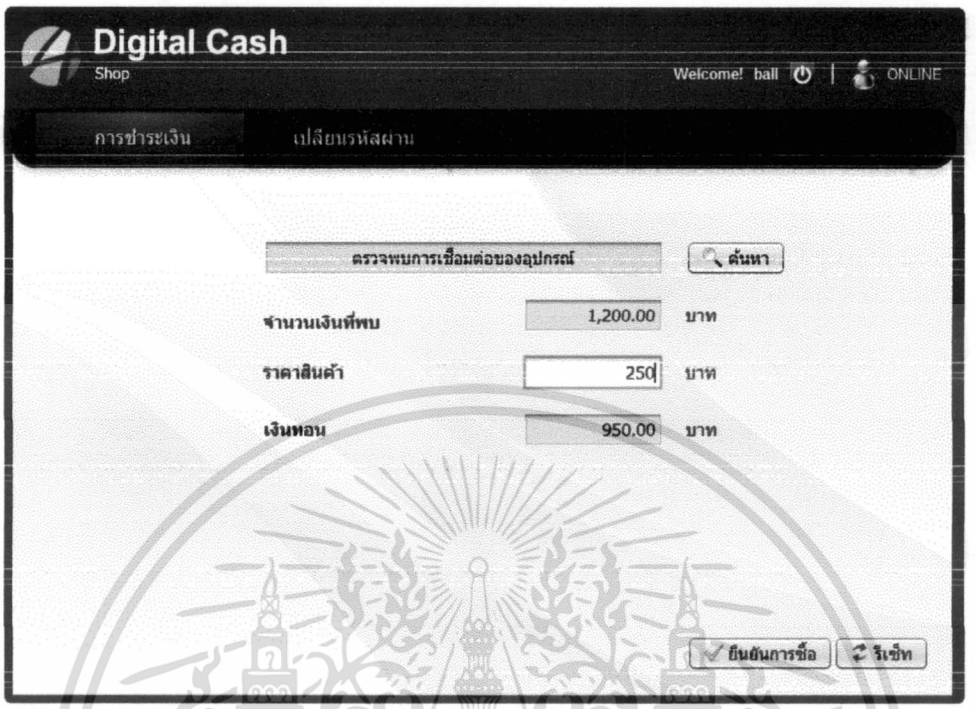
รูปที่ 4.14 แสดงตัวเลือกการขึ้น โดยการโอนเข้าบัญชี

4.3.2 ส่วนของระบบสำหรับร้านค้า

1. การเข้าใช้ระบบ แสดงดังรูปที่ 4.15

รูปที่ 4.15 หน้าต่าง Login เข้าใช้ระบบเงินสดดิจิตอลสำหรับร้านค้า

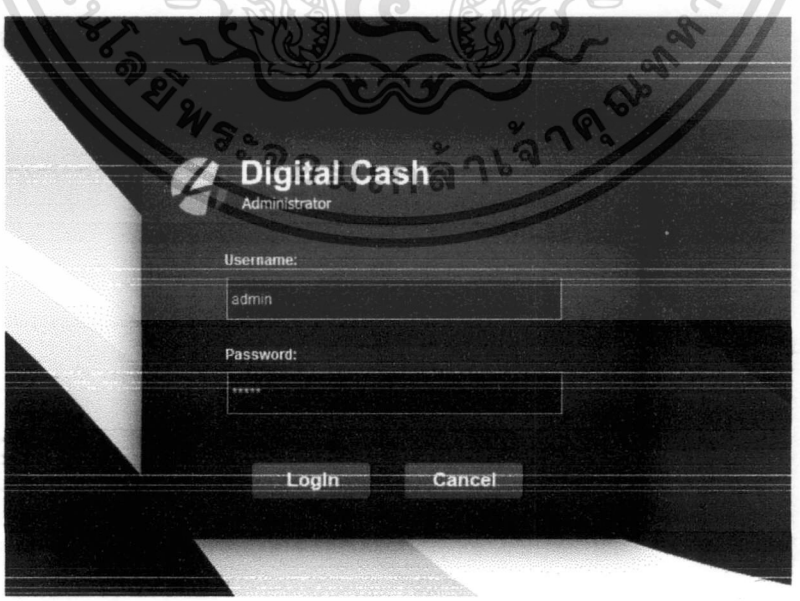
2. การซื้อขายสินค้า หรือบริการ แสดงดังรูปที่ 4.16



รูปที่ 4.16 การชำระเงิน

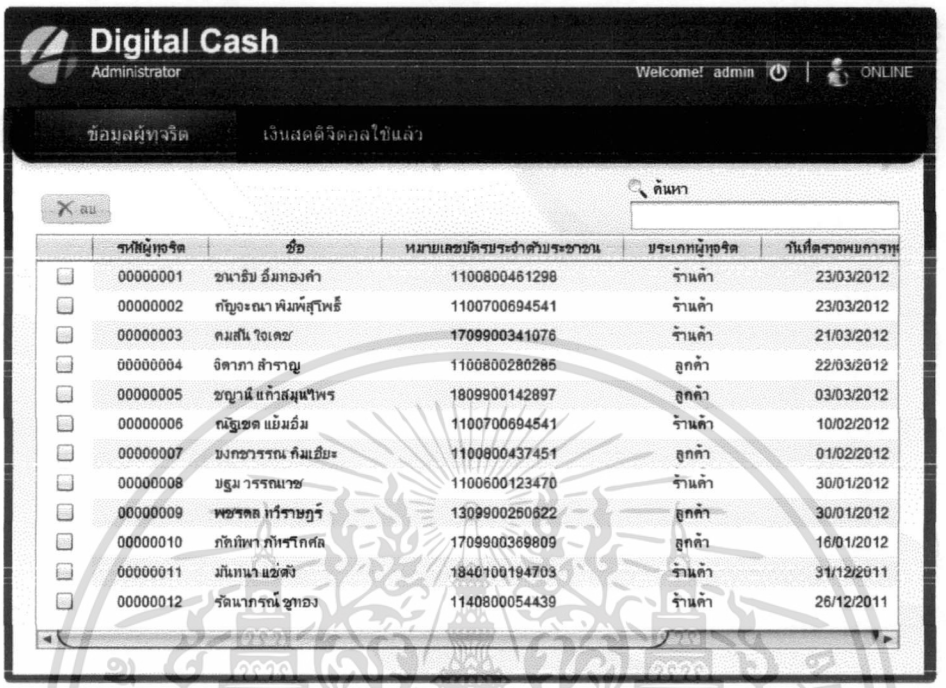
4.3.3 ส่วนของระบบสำหรับธนาคาร

1. การเข้าใช้ระบบ แสดงดังรูปที่ 4.17

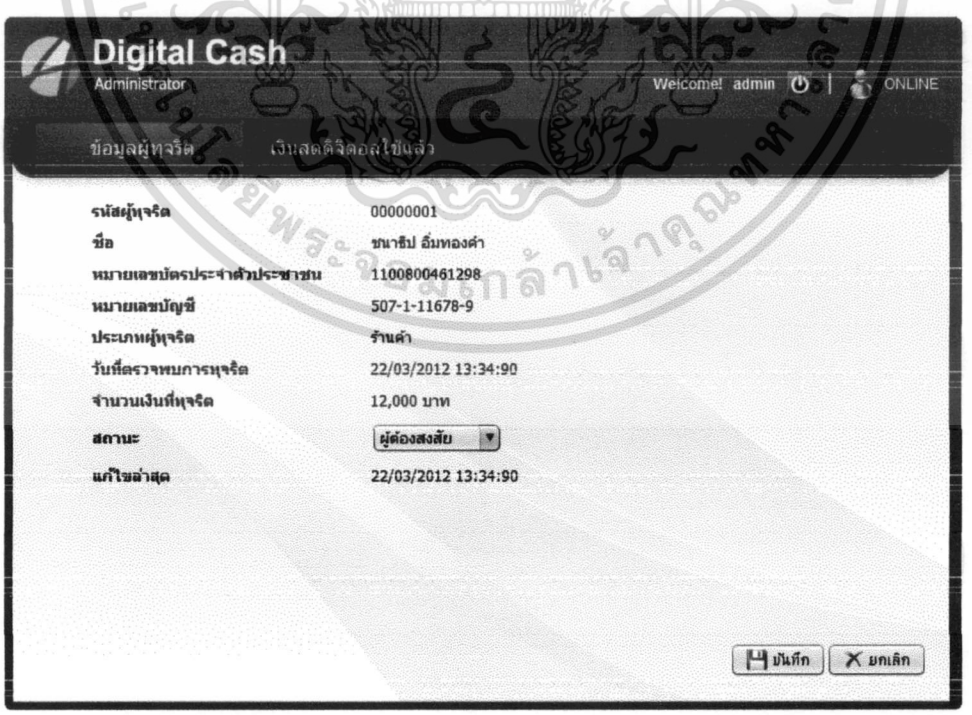


รูปที่ 4.17 หน้าต่าง Login เข้าใช้ระบบเงินสดดิจิตอลสำหรับผู้ดูแลระบบ

2. แสดงรายการผู้ทุจริต แสดงดังรูปที่ 4.18 และรูปที่ 4.19

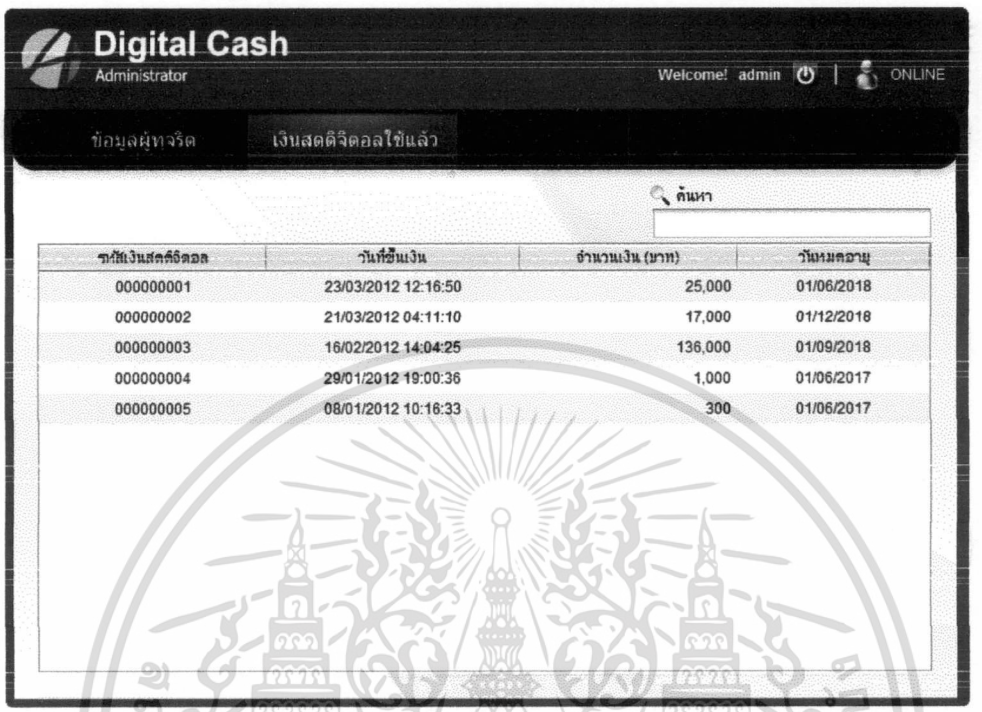


รูปที่ 4.18 รายการผู้ทุจริต



รูปที่ 4.19 รายละเอียดผู้ทุจริต

3. แสดงรายการเงินสดดิจิตอลใช้แล้ว แสดงดังรูปที่ 4.20



รูปที่ 4.20 รายการเงินสดดิจิตอลใช้แล้ว

บทที่ 5
บทสรุป และข้อเสนอแนะ

5.1 สรุปผลของโครงงาน

ระบบเงินสดดิจิตอลชนิดออฟไลน์นี้ เริ่มต้นจากการศึกษาทฤษฎีต่างๆที่เกี่ยวข้องกับวิทยาการการเข้ารหัสลับ ทฤษฎีที่เกี่ยวข้องกับระบบเงินสดดิจิตอล รวมถึงโพรโตคอลการทำงานของเงินสดดิจิตอล แล้วนำความรู้ที่ได้มาออกแบบระบบ และพัฒนาระบบขึ้นตามสิ่งได้ออกแบบไว้ โดยระบบเงินสดดิจิตอลชนิดออฟไลน์ที่พัฒนาขึ้นมีคุณสมบัติดังนี้

- ระบบแลกเปลี่ยนเงินสดดิจิตอล
  1. การซื้อเงิน
     - สามารถซื้อเงิน หรือเปลี่ยนเงินสดเป็นเงินสดดิจิตอลได้
     - สามารถตรวจสอบการซื้อเงินสดดิจิตอลในแต่ละวันได้
     - สามารถตรวจสอบการเชื่อมต่อของอุปกรณ์บันทึกข้อมูลได้
  2. การคืนเงิน หรือขึ้นเงิน
     - สามารถคืนเงิน หรือขึ้นเงิน หรือการเปลี่ยนเงินสดดิจิตอล เป็นเงินสดได้
     - สามารถตรวจสอบวันหมดอายุของเงินสดดิจิตอลได้
     - สามารถตรวจสอบการใช้เงินสดดิจิตอลซ้ำได้ และระบุได้ว่าใครเป็นผู้ทุจริต
     - สามารถติดต่อกับฐานข้อมูล เพื่อเพิ่มข้อมูลผู้ทุจริตลงในฐานข้อมูลผู้ทุจริตได้เมื่อตรวจพบการทุจริต และเพิ่มข้อมูลเงินสดดิจิตอลใช้แล้วลงในฐานข้อมูลเงินสดดิจิตอลใช้แล้วได้เมื่อมีการคืนเงิน หรือขึ้นเงิน
     - สามารถตรวจสอบการเชื่อมต่อของอุปกรณ์บันทึกข้อมูลได้

- ระบบเงินสดดิจิตอลสำหรับร้านค้า
  1. การชำระค่าสินค้า หรือบริการ
     - สามารถตรวจสอบความถูกต้องของเงินสดว่าถูกออกโดยธนาคารหรือไม่ได้
     - สามารถตรวจสอบวันหมดอายุของเงินสดดิจิตอลได้
     - สามารถคำนวณเงินทอนในขั้นตอนการชำระสินค้าได้
     - สามารถตรวจสอบการเชื่อมต่อของอุปกรณ์บันทึกได้
  2. การจัดการรหัสผ่าน
     - สามารถเปลี่ยนรหัสผ่านการเข้าใช้งานระบบได้

- ระบบเงินสดดิจิตอลสำหรับผู้ดูแลระบบ
  1. การจัดการกับเงินสดดิจิตอลใช้แล้ว
     - สามารถแสดงรายการเงินสดดิจิตอลใช้แล้วจากฐานข้อมูลได้
     - สามารถค้นหาข้อมูลด้วยคีย์เวิร์ด (Keyword) ได้
  2. การจัดการกับผู้ทุจริต
     - สามารถแสดงรายการผู้ทุจริตโดยการดึงข้อมูลจากฐานข้อมูลได้
     - สามารถค้นหาข้อมูลด้วยคีย์เวิร์ดได้
     - สามารถการปรับปรุงสถานะของข้อมูลผู้ทุจริต และลบข้อมูลผู้ทุจริตได้

ระบบเงินสดดิจิตอลชนิดออฟไลน์ มีข้อจำกัดของระบบมากกว่าชนิดออนไลน์ เนื่องจากกระบวนการทำงานที่ไม่สามารถตรวจสอบเงินสดดิจิตอลได้ในขณะที่ผู้ใช้ นำเงินสดดิจิตอลมาชำระเงิน ทำให้การติดตามตัวผู้ทุจริตทำได้ช้า เมื่อเกิดเหตุการณ์การทุจริตขึ้น แต่ถึงอย่างไรก็ตามระบบเงินสดดิจิตอลแบบออฟไลน์ที่พัฒนาขึ้นนี้ สามารถตรวจสอบผู้ทุจริตโดยสามารถระบุตัวผู้ทุจริตได้ แนวคิดในการกำหนดวงเงินสำหรับการซื้อเงินสดดิจิตอล เพื่อลดโอกาสการเกิดหนี้สูญ การออกแบบให้มีส่วนติดต่อกับผู้ใช้ที่คล้ายคลึงกับระบบเอทีเอ็มในปัจจุบัน เพื่อให้ง่ายต่อการใช้งาน สิ่งเหล่านี้สามารถเอื้อประโยชน์ในการเป็นต้นแบบของการพัฒนาระบบเงินสดดิจิตอล ที่อาจจะถูกพัฒนาขึ้นในลักษณะออนไลน์ และทำการรวมเข้ากับระบบเอทีเอ็มจริง ทำให้เกิดความสมบูรณ์ของระบบได้มากขึ้น

5.2 ปัญหาและอุปสรรค

1. เนื่องจากเป็นระบบที่ให้ความสำคัญกับการรักษาความลับของข้อมูล ทำให้ระบบมีความซับซ้อนกว่าปกติ
2. การพัฒนาระบบด้านความปลอดภัยเป็นความรู้ใหม่ของผู้พัฒนา ทำให้ต้องใช้เวลาในการศึกษา และทดลองใช้
3. ระบบเงินสดดิจิตอลชนิดออฟไลน์นี้ ประกอบด้วย 3 ระบบย่อย ทำให้ต้องใช้เวลาในการพัฒนา

5.3 ข้อเสนอแนะ และแนวทางการพัฒนาในอนาคต

1. ศึกษาเพิ่มเติมถึงความเป็นไปได้ในการพัฒนาให้ระบบเงินสดดิจิตอลให้มีคุณสมบัติการถ่ายโอน เพื่อให้สามารถนำเงินสดดิจิตอลที่ใช้แล้วไปใช้ต่อได้

2. นำต้นแบบระบบเงินสดดิจิตอลชนิดออฟไลน์นี้มาประยุกต์ให้เป็นแบบออนไลน์ เพื่อเพิ่มความสามารถของระบบ เช่น การตรวจสอบทุจริตที่ระบบของร้านค้า เป็นต้น
3. ศึกษาความเป็นไปได้ในการรวมระบบเงินสดดิจิตอลนี้เข้ากับระบบตู้เอทีเอ็ม เพื่อเป็นบริการเสริมอย่างหนึ่ง
4. เพิ่มฟังก์ชันการทำงานที่เกี่ยวข้องกับธุรกิจ เช่น การคิดค่าธรรมเนียมผู้นำเงินสดดิจิตอลหมดอายุมาคืนเงิน หรือขึ้นเงิน เพื่อเอื้อประโยชน์ด้านธุรกิจให้กับธนาคาร การสะสมคะแนนจากการใช้จ่ายผ่านระบบเงินสดดิจิตอล เพื่อกระตุ้นการใช้บริการ
5. พัฒนาเพื่อให้สามารถทำงานได้บนอุปกรณ์มือถือ เช่น อุปกรณ์มือถือประเภทสมาร์ตโฟน (Smart Phone) เพื่อเพิ่มความยืดหยุ่นของระบบ

บรรณานุกรม

ธนา หงษ์สุวรรณ. 2547. **"Secret Key"** [ออนไลน์]. เข้าถึงได้จาก: www.msne.mut.ac.th/member/filemanager/.../Secret%20Key.doc.

นิรนาม. 2551. **"การเข้ารหัสแบบ RSA"** [ออนไลน์]. เข้าถึงได้จาก: http://writesara.wordpress.com/2008/04/10/%e0%b8%81%e0%b8%b2%e0%b8%a3%e0%b9%80%e0%b8%82%e0%b9%89%e0%b8%b2%e0%b8%a3%e0%b8%ab%e0%b8%b1%e0%b8%aa%e0%b9%81%e0%b8%9a%e0%b8%9a-rsa/.

บรรจง หะรังษี. 2547. **"ความรู้เบื้องต้นของการเข้ารหัสข้อมูล (Introduction to Cryptography)"** [ออนไลน์]. เข้าถึงได้จาก: http://www.oknation.net/blog/admin-aristotle/2008/04/08/entry-2.

Anonymous. 2010. **"Conventional Cryptography"** [Online]. Available: http://dralu.com/?p=367.

Anonymous. 2012. **"Conventional Cryptography"** [Online]. Available: http://library.thinkquest.org/C0126342/secret.htm.

B. Schneier. 1996. **"Applied Cryptography"**. 2nd Ed. John Wiley & Sons, Inc.

D. Chaum, A. Fiat and N. Naor. 1990. **"Untraceable Electronic Cash"**. Springer-Verlag.

D. Chaum. Oct 1985. **"Security without Identification: Transaction Systems to Make Big Brother Obsolete"**. Communications of the ACM.

ประวัติผู้เขียน

ชื่อ	นายชนาธิป อิ่มทองคำ
วัน เดือน ปี เกิด	3 พฤษภาคม2530
ที่อยู่	เลขที่ 21ถนนดอนเหียงตำบลประจวบคีรีขันธ์ อำเภอเมือง ประจวบคีรีขันธ์ จังหวัดประจวบคีรีขันธ์ 77000
ประวัติการศึกษา	วิทยาศาสตรบัณฑิต สาขาเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง วิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีระบบสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง