



477-403 โครงการระบบสารสนเทศ 2

(Project in Information System II)

สุขภาพส่วนบุคคลที่มีความปลอดภัย

Secure Personal Health Care

จัดทำโดย

นาย ชัยสิทธิ์	แช่ม	รหัส 5910513007
นาย สันต์ทศน์	กาญจนนิธิสกุล	รหัส 5910513042
นาย ศิวกร	อภิสิทธิ์วงศ์	รหัส 5910513077

อาจารย์ที่ปรึกษา

ผู้ช่วยศาสตราจารย์จิรวรรณ ลำอางศรี

ภาคการศึกษาที่ 2 ปีการศึกษา 2561

ภาควิชาบริหารธุรกิจ หลักสูตรระบบสารสนเทศทางธุรกิจ

คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์

## คำนำ

รายงานฉบับนี้เป็นส่วนหนึ่งของวิชา 477-402 โปรเจก โดยมีจุดประสงค์เพื่อศึกษาเทคโนโลยี blockchain และนำเทคโนโลยี blockchain มาใช้พัฒนา web application โดย เว็บของเราคือ Personal health care system เป็นเว็บไซต์ขายประกันออนไลน์โดยจะเก็บประวัติการรักษาและประวัติส่วนตัวของผู้ป่วย โรคเบาหวานที่ซื้อประกันกับเราเพื่อติดตามผลการรักษาและสภาพร่างกายของผู้ป่วยร่วมไปถึงสร้างแรงจูงใจในการดูแลสุขภาพตนเอง โดยทั้งหมดจัดเก็บลงใน blockchain เพราะข้อมูลที่เป็นความลับเป็นเรื่องของความเป็นส่วนตัวควรใช้เทคโนโลยีที่มีความปลอดภัยให้มากที่สุด

คณะผู้จัดทำหวังว่า เนื้อหาในรายงานสัมมนานี้จะเป็นประโยชน์ต่อผู้ที่สนใจไม่มากนักน้อย หากรายงานฉบับนี้ผิดพลาดประการใด ต้องขอ อภัยไว้ ณ โอกาสนี้ด้วย

คณะผู้จัดทำ

## สารบัญ

คำนำ	ก
สารบัญ	๗
สารบัญรูปภาพ	ค
บทที่ 1 บทคัดย่อ	1
บทที่ 2 แนวคิด และ ทฤษฎี	2
โรคเบาหวาน	3
โรคเบาหวานน่ากลัวอย่างไร	6
Blockchain คืออะไร	7
ทำความรู้จักกับ Ethereum และ Smart Contract	8
ความเป็นส่วนตัว (Privacy) บนเทคโนโลยีบล็อกเชน (Blockchain)	12
พัฒนาการของ Blockchain	13
เครื่องมือในการพัฒนา	19
บทที่ 3 การออกแบบ	26
โครงสร้างข้อมูล	26
ฟังก์ชันหลัก	29
บทที่ 4 ผลการดำเนินการ	30
บทที่ 5 สรุปผลการดำเนินงาน และข้อเสนอแนะ	33
บรรณานุกรม	34

## สารบัญรูปภาพ

ภาพที่ 1 ภาพแสดงบล็อกเชนที่มีจุดต่อกันยาวสุดตั้งแต่ต้นโดย	
บล็อกเริ่มต้นที่สี่เทาและบล็อกกำไรเป็นสีน้ำตาลและฟ้า	8
ภาพที่ 2 ภาพแสดงการเข้ารหัสลับแบบกุญแจสมมาตร	10
ภาพที่ 3 ภาพแสดงการเข้ารหัสลับแบบกุญแจสมมาตร	10
ภาพที่ 4 ภาพแสดงตัวอย่างในการคำนวณ Elliptic Curve	11
ภาพที่ 5 ภาพด้านซ้ายเป็นระบบ Payment ในปัจจุบันที่ต้องผ่านคนกลาง	
ภาพด้านขวาเป็นการทำธุรกรรมแบบ peer-to-peer ที่มีการบันทึก	
ข้อมูลรายการธุรกรรมทั้งหมดแบบกระจายศูนย์ (Decentralize)	13
ภาพที่ 6 พัฒนาการของ Blockchain	13
ภาพที่ 7 หน้าตาของ Remix Ide	19
ภาพที่ 8 Logo Metamask	19
ภาพที่ 9 หน้าเว็บ Metamask	20
ภาพที่ 10 คลิกรับส่วนขยาย	20
ภาพที่ 11 เพิ่ม Metamask ใน chrome	21
ภาพที่ 12 เพิ่ม Add extension Metamask ใน chrome	21
ภาพที่ 13 สังเกตมุมขวามือเมื่อติดตั้งสำเร็จ	22
ภาพที่ 14 คลิกเข้า Metamask	22
ภาพที่ 15 Get Started Metamask	23

ภาพที่ 16 สร้างหรือเข้าสู่ระบบ	23
ภาพที่ 17 สร้างรหัสผ่าน Metamask	24
ภาพที่ 18 การรับชุดคำยืนยันบัญชี	24
ภาพที่ 19 การยืนยันชุดคำ	25
ภาพที่ 20 struct user	26
ภาพที่ 21 struct result	27
ภาพที่ 22 struct pressure	27
ภาพที่ 23 struct fat	27
ภาพที่ 24 struct pay	29
ภาพที่ 25 หน้าสมัครสมาชิก	30
ภาพที่ 26 Login	30
ภาพที่ 27 การแสดงข้อมูลผู้ใช้	31
ภาพที่ 28 การบันทึกข้อมูลผลการตรวจ	31
ภาพที่ 29 ชำระค่าบริการด้วย Ethereum	32
ภาพที่ 30 แสดงข้อมูลการตรวจและสถานะของโรค	32

## บทที่ 1 บทคัดย่อ

ปัจจุบันมีประชากรที่ตายก่อนวันอันควรด้วยโรคไม่ติดต่อที่สำคัญ 4 ได้แก่ โรคความดันโลหิตสูง โรคเบาหวาน โรคหัวใจขาดเลือด และโรคหลอดเลือดสมองซึ่งในแต่ละโรคสามารถรักษาได้แต่ไม่สามารถหายขาดจากโรคนั้นได้จัดว่าเป็นโรคเรื้อรังที่ต้องรักษาอาการให้อยู่ในสถานะสมดุลมีการดูแลมีการดูแลตัวเองอย่างต่อเนื่องหรือจากบุคคลรอบข้างเพื่อให้สภาวะของโรคไม่ร้ายแรง เบาหวานเป็น 1 ใน 4 โรคยอดฮิตที่มักเกิดในผู้สูงอายุแต่ไม่ได้หมายความว่าเด็กจะไม่มีอัตราการเกิดซึ่งผู้สูงอายุจะต้องดูแลทั้งสภาพร่างกาย อาหารการกิน รวมไปถึงการกินยาเพื่อควบคุมระดับน้ำตาล ความดัน ฯลฯ และหนึ่งในสาเหตุที่ทำให้อาการเหล่านี้แย่หรือทรุดลงก็คือการไม่ออกกำลังกาย รักษาหลายอาการหาที่รับประทานมีผลขัดแย้งกัน รวมไปถึงการไม่ทราบถึงระดับความร้ายแรงของอาการตนเองและเกิดการปล่อยปะละเลยไม่ได้ดูแลอย่างต่อเนื่องและหากไม่มีประกันชีวิตค่ารักษาพยาบาลต่อไปจะเป็นภาระใหญ่สำหรับครอบครัวหรือตัวผู้ป่วยเอง

ระบบ Personal Health Care System เป็นระบบดูแลสุขภาพส่วนบุคคล มาจาก Personal Health Care ที่แปลว่าการบริการสุขภาพส่วนบุคคล นำมาถึงการใช้งานผ่านระบบ Web application ช่วยให้ได้รับการรักษาได้รวดเร็วจากข้อมูลที่ไม่ต้องรอฟังเรื่องขอจากต่างโรงพยาบาล เตือนถึงสภาวะของโรคที่กำลังเป็นอยู่ว่าจุดไหนควรระวังเป็นพิเศษเพื่อให้ดูแลเน้นย้ำในจุดนั้นได้โดยนำข้อมูลจากผู้ใช้โดยระบบจะสามารถบันทึกข้อมูลผลการรักษาในแต่ละครั้งได้และนำข้อมูลนั้นมาวิเคราะห์กับค่ามาตรฐานที่ควรจะเป็นเพื่อแจ้งเตือนผู้ใช้งานเพื่อเป็นการเตือนความจำ และ สุดท้ายระบบ จะมาพร้อมประกันสุขภาพ สำหรับผู้ที่เป็นโรคเบาหวานเพื่อช่วยเป็นหนึ่งช่องทางการออมเงินเพื่อไว้ใช้จ่ายในค่ารักษาพยาบาลและข้อมูลข้างต้นยังมีประโยชน์ในสถานะการฉุกเฉินก็คือไม่ว่าท่านจะอยู่ที่ไหนรักษาที่โรงพยาบาลใดข้อมูลมูลในระบบจะช่วยลดขั้นตอนการทำงานขอแพทย์ลงเพราะถือเป็นประวัติการรักษาได้เช่นกัน ซึ่งระบบมาพร้อมกับการรักษาความปลอดภัยโดยใช้ Blockchain มาพัฒนาทั้งหมด เพื่อให้ข้อมูลส่วนตัวของลูกค้ามีความปลอดภัยจากการโจรกรรมและไม่ต้องกังวลว่าทางเจ้าของระบบจะนำข้อมูลไปใช้ทำอย่างอื่นอย่างใด

Personal Health Care System ระบบดูแลสุขภาพส่วนบุคคล สำหรับคนที่เป็นเบาหวานที่มาพร้อมกับประกันสุขภาพเป็นระบบที่มีความปลอดภัยสูงเนื่องจากพัฒนาด้วย Blockchain และ ไม่มีคนกลางหรือ amind คนดูแลโดยจะใช้ Smart contract เป็นตัวงานอัตโนมัติในระบบทำให้ปลอดภัยไม่รั่วไหลแน่นอน

## บทที่ 2 แนวคิด ทฤษฎีที่เกี่ยวข้องและเครื่องมือที่ใช้ในการพัฒนาระบบดูแลสุขภาพตัวเอง PCH

ระบบสุขภาพ (Health System) หมายถึง ระบบความสัมพันธ์ทั้งหมดที่เกี่ยวข้อง กับสุขภาพ (มาตรา ๓ พ.ร.บ.สุขภาพแห่งชาติ พ.ศ. ๒๕๕๐) ซึ่งมีผลลัพธ์ที่สำคัญ คือ การเข้าถึง ความครอบคลุม คุณภาพ ความปลอดภัย และมีผลสัมฤทธิ์ที่ทำให้ประชาชน มีระดับสุขภาพและความเป็นธรรมเชิงสุขภาพที่ดีขึ้น มีประสิทธิภาพ คุ้มครองความเสี่ยง ทั้งด้านสังคมและการเงิน และตอบสนองต่อความคาดหวังของประชาชน โดยระบบ สุขภาพประกอบด้วยองค์ประกอบพื้นฐานอย่างน้อย ๖ ประการ ได้แก่ ๑) การให้บริการ สุขภาพ ๒) บุคลากรสุขภาพ ๓) สารสนเทศสุขภาพ ๔) ผลิตภัณฑ์ทางการแพทย์ วัคซีน และ เทคโนโลยี ๕) การเงินการคลัง สุขภาพ ๖) ภาวะผู้นำและการอภิบาล (รายละเอียด เอกสารสมัชชาสุขภาพ ๘ / หลัก ๓ / แผนก ๑) ระบบ

บริการสุขภาพ (Health Care Systems/Health Service Systems) หมายถึง แบบแผนของการจัดบริการสุขภาพ จัดเป็นองค์ประกอบหนึ่งของระบบสุขภาพ มักจะใช้ เพื่อหมายถึงระบบหรือโครงการจัดบริการสุขภาพ ให้แก่ประชาชนหรือสาธารณะ โดยการ ลงทุนของรัฐหรือหน่วยงานเอกชนหรือร่วมกันทั้งสองภาคส่วน ประกอบด้วยกิจกรรม ต่าง ๆ ทั้งในด้านการส่งเสริมสุขภาพ การป้องกันโรค การรักษาพยาบาลและการฟื้นฟู 8.indd 74 8/2/2559 13:45:34 มติสมัชชาสุขภาพแห่งชาติ ครั้งที่ ๘ 75 สุขภาพ และในความหมายที่กว้าง องค์ประกอบของระบบบริการสุขภาพจะครอบคลุม ถึงดังต่อไปนี้ ๑) บริการดูแลสุขภาพรายบุคคลของบุคคล และครอบครัว ใช้บริการได้ ตามโรงพยาบาล คลินิก ศูนย์สุขภาพในชุมชน ในสำนักงานแพทย์ และในบ้านของ ผู้รับบริการเอง ๒) บริการสาธารณสุขซึ่งจำเป็นต่อการรักษาถึงแวดล้อมให้เอื้อต่อสุขภาพ เช่นการควบคุม นำอาหารและยา และกฎความปลอดภัยต่าง ๆ ที่มุ่งปกป้องประชากร กลุ่มใดกลุ่มหนึ่ง ๓) กิจกรรมฝึกอบรมสอน และและวิจัยใด ๆ ที่เกี่ยวข้องกับการป้องกันโรค การค้นหาผู้ป่วยและการรักษาโรค และ ๔) การเรียกเก็บ ค่าบริการจากบุคคลภายนอก เช่น จากระบบประกันสุขภาพ

เมื่อนำ บริการสุขภาพ (Health Care Systems/Health Service Systems) มารวมกับคำว่า Personal จึง นิยามได้ว่า การบริการสุขภาพส่วนบุคคล (Personal Health Care System) คือการบริการสุขภาพตนเองด้วย ตนเองโดยเอาแนวคิดจากระบบ Health Cere ที่ต่างประเทศนำมาประยุกต์ให้อยู่ในรูปแบบ web application เพื่อให้ผู้ใช้งานสามารถเข้าถึงได้ทุกที่ทุกเวลาและได้รับสิทธิประโยชน์ด้านการออมทรัพย์เพื่อใช้เป็นค่าใช้จ่ายในการรักษาและเป็นสื่อกลางระหว่างผู้ใช้กับโรงพยาบาลหรือคลินิกต่างๆในเรื่องประวัติการรักษาเพื่อลดโอกาส ในการเกิดความผิดพลาดในการให้ข้อมูลหรือประวัติทางการแพทย์และลดขั้นตอนในการซักถามประวัติคนไข้ หรือขอประวัติการรักษาจากโรงพยาบาลก่อนหน้า

## โรคเบาหวาน

**โรคเบาหวาน (Diabetes Mellitus: DM)** เป็นภาวะที่ร่างกายมีน้ำตาลในเลือดสูงกว่าปกติ เนื่องจากการขาดฮอร์โมนอินซูลิน (Insulin) หรือการดื้อต่อฮอร์โมนอินซูลิน ส่งผลให้กระบวนการดูดซึมน้ำตาลในเลือดให้เป็นพลังงานของเซลล์ในร่างกายมีความผิดปกติหรือทำงานได้ไม่เต็มประสิทธิภาพ จนเกิดน้ำตาลสะสมในเลือดปริมาณมาก หากปล่อยให้ร่างกายอยู่ในสภาวะนี้เป็นเวลานานจะทำให้มีภาวะต่าง ๆ เสื่อม เกิดโรคและอาการแทรกซ้อนขึ้น

จากข้อมูลของสหพันธ์เบาหวานนานาชาติ (International Diabetes Federation: IDF) พบผู้ป่วยโรคเบาหวานทั่วโลก 425 ล้านคนในปี 2560 และคาดการณ์ว่าจะมีจำนวนผู้ป่วยด้วยโรคนี้มากถึง 629 ล้านคนในปี 2588 สำหรับสถานการณ์โรคเบาหวานในประเทศไทยพบว่า คนไทยช่วงอายุ 20-79 ปี เป็นโรคเบาหวานร้อยละ 8.3 หรือหมายความว่าใน 100 คน จะพบคนที่ป่วยเป็นโรคเบาหวานประมาณ 8 คน และจำนวนมากกว่าครึ่งไม่ทราบว่าตนเองเป็นโรคเบาหวาน สถิติการพบผู้ป่วยด้วยโรคนี้ยังมีจำนวนมากขึ้นเรื่อย ๆ จนทำให้ต้องมีการรณรงค์อย่างต่อเนื่องถึงภัยร้ายของโรค เพราะเป็นโรคเรื้อรังที่รักษาไม่หายขาด มีโอกาสเสี่ยงต่อโรคแทรกซ้อนลุกลามใหญ่โตจนต้องสูญเสียอวัยวะที่สำคัญของร่างกาย ทางสหพันธ์เบาหวานนานาชาติ และองค์การอนามัยโลก (WHO) จึงได้กำหนดให้วันที่ 14 พฤศจิกายนของทุกปีเป็นวันเบาหวานโลก เพื่อให้ตระหนักถึงความสำคัญของโรคนี้

ในปัจจุบัน ประเทศไทยยึดหลักเกณฑ์ตามสมาคมเบาหวานแห่งประเทศไทยในการจำแนกผู้ป่วยโรคเบาหวานด้วยการตรวจปริมาณน้ำตาลในเลือด หากผลการตรวจหลังอดอาหารและเครื่องดื่มน้ำตาลอยู่กระแสดเลือดไม่เกิน 100 มิลลิกรัมต่อเดซิลิตร แสดงว่าระดับน้ำตาลในเลือดปกติ ทั้งนี้ระดับน้ำตาลในเลือดยังบ่งบอกถึงภาวะเสี่ยงต่อการเป็นเบาหวานได้ด้วย (Prediabetes) ซึ่งผู้ที่อยู่ในกลุ่มเสี่ยงต่อภาวะเป็นเบาหวานสามารถพัฒนาการเกิดโรคเบาหวานประเภทที่ 2 (เบาหวานที่เกิดจากการที่ตับอ่อนผลิตฮอร์โมนอินซูลินได้ไม่เพียงพอต่อการใช้) โรคหัวใจ และโรคหลอดเลือดในสมองในอนาคตได้ง่ายขึ้น

### อาการของโรคเบาหวาน

โรคเบาหวานในระยะแรกจะไม่แสดงอาการผิดปกติ บางรายอาจตรวจพบโรคเบาหวานเมื่อพบภาวะแทรกซ้อนขึ้นแล้ว อาการของโรคเบาหวานแต่ละชนิดอาจมีความคล้ายกัน ซึ่งอาการที่พบส่วนใหญ่ คือ กระหายน้ำมาก ปากแห้ง ปัสสาวะบ่อย หิวบ่อย น้ำหนักลดหรือเพิ่มผิดปกติ สายตาพร่ามัว เห็นภาพไม่ชัด รู้สึกเหนื่อยง่าย มีอาการชา โดยเฉพาะมือและขา บาดแผลหายยาก เป็นต้น ทั้งนี้ อาการของโรคเบาหวานประเภทที่ 1 จะเกิดขึ้นอย่างรวดเร็ว ในขณะที่โรคเบาหวานประเภทที่ 2 จะแสดงอาการแบบค่อยเป็นค่อยไป ส่วนโรคเบาหวานขณะตั้งครรภ์มักเกิดขึ้นในช่วงอายุครรภ์ประมาณ 24-28 สัปดาห์



## สาเหตุของโรคเบาหวาน

โรคเบาหวานมีหลายประเภท สามารถแบ่งออกได้เป็น 3 ประเภท คือ เบาหวานประเภทที่ 1 (Type 1 Diabetes) เกิดจากตับอ่อนไม่สามารถผลิตฮอร์โมนอินซูลินได้ เบาหวานประเภทที่ 2 (Type 2 Diabetes) เกิดจากการที่ตับอ่อนผลิตฮอร์โมนอินซูลินได้ไม่เพียงพอต่อการใช้ หรือเกิดภาวะการดื้ออินซูลิน (Insulin Resistance) และ เบาหวานขณะตั้งครรภ์ (Gestational Diabetes) ซึ่งเป็นโรคเบาหวานที่พัฒนาขึ้นระหว่างการตั้งครรภ์จากการเปลี่ยนแปลงฮอร์โมน โดยที่ผู้ป่วยไม่เคยเป็นโรคเบาหวานมาก่อน

นอกจากโรคเบาหวานทั้ง 3 ประเภทแล้วยังมีโรคเบาหวานที่พบได้ไม่บ่อยอย่างโรคเบาหวานที่เกิดจากกรรมพันธุ์หรือแบบโมโนเจนิค (Monogenic Diabetes) อีกทั้งยังมีโรคเบาหวานจากสาเหตุอื่น ๆ เช่น การใช้ยา หรือเกิดจากโรคชนิดอื่นอย่าง โรคซิสติก ไฟโบรซิส (Cystic Fibrosis) ด้วย

## การวินิจฉัยโรคเบาหวาน

แพทย์จะสอบถามอาการผู้ป่วย ประวัติการเจ็บป่วยของผู้ป่วยและของบุคคลในครอบครัว และการตรวจร่างกาย และที่สำคัญต้องอาศัยการตรวจเลือด เพื่อดูระดับน้ำตาลในเลือดเป็นหลัก โดยมีวิธีการวิเคราะห์ระดับน้ำตาลในเลือดหลายวิธี ได้แก่

- การตรวจระดับน้ำตาลในเลือดเวลาใดก็ได้ (Random/Casual Plasma Glucose Test)
- การตรวจระดับน้ำตาลในเลือดหลังอดอาหารอย่างน้อย 8 ชั่วโมง (Fasting Plasma Glucose: FPG)
- การตรวจน้ำตาลเฉลี่ยสะสม หรือฮีโมโกลบิน เอ วัน ซี (Hemoglobin A1c: HbA1c)
- การทดสอบการตอบสนองของฮอร์โมนอินซูลินต่อระดับน้ำตาลในเลือด (Oral Glucose Tolerance Test: OGTT)

หากผู้ป่วยไม่มีอาการของโรคเบาหวานชัดเจน คือ หิวน้ำมาก ปัสสาวะบ่อยและมาก น้ำหนักตัวลดลง โดยที่ไม่มีสาเหตุ การตรวจด้วยวิธีทั้งหมดข้างต้นจำเป็นต้องมีการตรวจซ้ำอย่างน้อย 1 ครั้งด้วยวิธีใดวิธีหนึ่งอีกครั้งหนึ่ง เพื่อยืนยันผลการวินิจฉัย

## การรักษาโรคเบาหวาน

การรักษาผู้ป่วยเบาหวานในประเภทที่ 1 จำเป็นต้องได้รับฮอร์โมนอินซูลินเข้าไปทดแทนในร่างกายด้วยการฉีดยาเป็นหลัก ควบคู่ไปกับการคุมอาหารและออกกำลังกายที่เหมาะสม ในขณะที่โรคเบาหวานประเภทที่ 2 หากเป็นในระยะแรก ๆ สามารถรักษาได้ด้วยการรับประทานอาหารที่เหมาะสม การออกกำลังกาย และควบคุมน้ำหนัก หากอาการไม่ดีขึ้น แพทย์อาจให้ยาควบคู่ไปด้วยหรือฉีดอินซูลินเข้าไปทดแทนเช่นเดียวกับโรคเบาหวานชนิดที่ 1

สำหรับผู้เป็นโรคเบาหวานขณะตั้งครรภ์ ควรเข้าฝากครรภ์กับแพทย์ตั้งแต่ในระยะแรก พร้อมทั้งควบคุมอาหารที่รับประทานและออกกำลังกายตามคำแนะนำของแพทย์

นอกจากนี้ ในกรณีที่ผู้ป่วยเกิดแผลเบาหวานขึ้นที่เท้า แพทย์อาจให้ผู้ป่วยใส่อุปกรณ์ป้องกันแผล เช่น รองเท้า สำหรับผู้ป่วยเบาหวาน ฝ่าเท้า หรือฝ่าเท้าแบน เป็นต้น หากแผลเริ่มมีลักษณะรุนแรงขึ้น แพทย์อาจวางแผนการรักษาตามเหมาะสมขึ้นอยู่กับระดับความรุนแรงของแผลเบาหวานที่เป็น ทั้งนี้ หากรักษาแล้วอาการไม่ดีขึ้น แพทย์อาจต้องตัดอวัยวะทิ้งเพื่อป้องกันอาการลุกลาม

สำหรับผู้ที่เป็นโรคเบาหวานจะต้องเฝ้าดังนี้

- ระดับน้ำตาลในเลือด (FPG) 70-130 มก./ดล. (ถ้าน้อยกว่า 70 หรือมากกว่า 150 ต้องปรับเปลี่ยนการดูแลรักษาเพิ่มเติม)
- ระดับน้ำตาลเฉลี่ยในเลือด (HbA1C) มีค่าน้อยกว่า 7.0% (ถ้ามากกว่า 8% ต้องปรับเปลี่ยนการดูแล)
- ความดันต่อน้อย 130/80 มม.ปรอท
- ระดับไขมันในเลือด โดยมี
  - ระดับไตรกลีเซอไรด์ (TG) ต่ำน้อยกว่า 150 มก./ดล.,
  - แอลดีแอล (LDL) น้อยกว่า 100 มก./ดล.
  - เอชดีแอล (HDL) ในผู้ชายมากกว่า 40 มก./ดล. ส่วนผู้หญิงมากกว่า 50 มก./ดล.
- สารไข่ขาว (Albumin) ในปัสสาวะ มีค่าน้อยกว่า 30 มก./ลิตร
- ดัชนีมวลกายอยู่ที่ 18.5-22.9 กก./ม.2

## ภาวะแทรกซ้อนของโรคเบาหวาน

โรคเบาหวานเป็นโรคที่ส่งผลให้ผู้ป่วยมีระดับน้ำตาลในเลือดสูงมากกว่าปกติ หากไม่มีการควบคุมในเรื่องของการรับประทานอาหารและดูแลรักษาสุขภาพอย่างถูกวิธี ปล่อยให้ระดับน้ำตาลในเลือดสูงขึ้นเป็นเวลานาน จะส่งผลต่อเส้นเลือดที่นำสารอาหารไปเลี้ยงอวัยวะในร่างกายจนนำไปสู่ภาวะแทรกซ้อนต่าง ๆ ทั้งโรคแทรกซ้อนชนิดที่เกิดกับเส้นเลือดขนาดเล็ก เช่น เบาหวานขึ้นตา โรคไต เป็นต้น หรือโรคแทรกซ้อนชนิดที่เกิดกับเส้นเลือดขนาดใหญ่ เช่น โรคหัวใจ โรคหลอดเลือดสมอง โรคเส้นเลือดแดงส่วนปลายอุดตัน เป็นต้น รวมไปถึงโรคแทรกซ้อนที่ระบบประสาทและที่สามารถทำให้ผู้ป่วยต้องสูญเสียอวัยวะบางส่วน นอกจากนี้สตรีมีครรภ์ที่เป็นโรคเบาหวานจะเพิ่มความเสี่ยงต่อภาวะครรภ์เป็นพิษ การแท้งบุตรได้

## โรคเบาหวานน่ากลัวอย่างไร

อย่างที่ทราบกันดีว่าในตอนนี้ทั่วโลกต้องเจอกับโรค Covid-19 หรือโรคไข้หวัดใหญ่สายพันธุ์ใหม่ แต่หากว่า Covid-19 อันตรายแล้วก็ต้องขอบอกว่า เรื่องของโรคเบาหวานนั้นยิ่งน่ากลัวกว่าอีกหลายเท่า แม้จะไม่ใช่โรคติดต่อ แต่ผมต้องขอนามกล่าวถึงเป็นพิเศษ เพราะเดิมทีผมไม่เคยเข้าใจว่าเป็นโรคที่อันตรายอย่างมาก หลายคนคงจะเข้าใจเหมือนกับผมว่า โรคหัวใจ-ความดันโลหิตสูงเป็นโรคที่อันตราย แต่หลายคนรวมทั้งผม นั้นจะไม่ค่อยกลัวโรคเบาหวานเท่าที่ควร ผมจึงขอเสนอข้อมูลจากองค์การอนามัยโลก และ International Diabetes Federation ดังนี้

- มีคนเสียชีวิตจากโรคเบาหวานทั่วโลก 1.6 ล้านคน ในปี 2016 และปัจจุบันจำนวนผู้เสียชีวิตน่าจะใกล้ 2 ล้านคนต่อปีแล้ว หากประเมินจากแนวโน้มการเพิ่มขึ้นของโรคนี้ในอดีต

- มีผู้ป่วยเป็นโรคเบาหวานทั่วโลก 464 ล้านคน ในปี 2019 โดยประมาณ ผู้ใหญ่มีสัดส่วนเป็นโรคเบาหวานประมาณ 9.3% และคาดการณ์ว่า จำนวนผู้เป็นโรคเบาหวานทั่วโลกจะเพิ่มขึ้นเป็น 629 ล้านคน ในปี 2045 หากนำเอาส่วนต่างของตัวเลขทั้งสองไปหารด้วยจำนวนปีก็จะได้ตัวเลขที่พอสรุปได้ว่า จะมีผู้เป็นโรคเบาหวานเพิ่มขึ้นบนโลกในปีละ 6.34 ล้านคน ใน 26 ปีข้างหน้า ซึ่งจะทำให้การแพร่ขยายของโรค COVID-19 คุณเป็นเรื่องที่เล็กน้อยกว่าโรคเบาหวานอย่างมาก

- 79% ของผู้ใหญ่ที่เป็นโรคเบาหวานอาศัยอยู่ในประเทศที่มีรายได้ปานกลางและรายได้ต่ำ (โรคเบาหวานไม่ใช่โรคของคนรวย)

- 50% ของผู้ที่เป็นโรคเบาหวาน (232 ล้านคน) ไม่ทราบว่าตัวเองเป็นโรคเบาหวานเพราะไม่ได้ไปตรวจเลือด

## Blockchain คืออะไร

**Blockchain** คือ ระบบโครงข่ายในการเก็บบัญชีธุรกรรมออนไลน์ ซึ่งมีลักษณะเป็นเครือข่ายแบบกระจายศูนย์ที่เก็บสถิติการทำธุรกรรมทางการเงิน และสินทรัพย์ชนิดอื่นๆ อีกในอนาคต โดยไม่มีตัวกลาง ระบบ Blockchain จะไม่มีตัวกลางอย่างที่เคยเป็นมา ยกตัวอย่างการทำธุรกรรมด้วย Bitcoin จะมีรหัส Token สร้างขึ้นมาเพื่อสื่อสารกับ Blockchain และทำการตรวจสอบว่า Bitcoin นั้นๆ มีความน่าเชื่อถือหรือไม่ก่อนที่จะทำธุรกรรมให้สำเร็จต่อไป

เท่ากับว่า Blockchain เป็นระบบโครงข่ายในการทำธุรกรรมต่างๆ ซึ่งตัดตัวกลางอย่างสถาบันการเงินที่มีอยู่ในโลกปัจจุบันออกไป ซึ่งทำให้ต้นทุนการทำธุรกรรมถูกลง และอาจจะส่งผลให้สถาบันการเงินที่เป็นตัวกลาง รวมไปถึงสำนักชำระบัญชีต่างๆ ไม่จำเป็นต้องมีอีกในอนาคตได้เลย หากเทคโนโลยีนี้เข้ามาแทนที่ได้อย่างสมบูรณ์ ขณะที่ Blockchain ไม่เพียงมีบทบาทอยู่แค่การทำธุรกรรมทางการเงินเท่านั้น หากแต่ยังอาจถูกนำไปใช้ในงานอื่นๆ เช่น การเก็บสถิติการเลือกตั้งให้มีความโปร่งใสมากขึ้น การให้ยืม Cloud Storage ระหว่างกัน, บริการ co-location, ระบบ Peer to Peer Lending และอื่นๆ อีกมากมาย ซึ่งแม้แต่เหล่าธนาคารเองก็ตัดสินใจเข้าลงทุนในการทำ Blockchain มากขึ้นเรื่อยๆ โดยล่าสุด เหล่าสถาบันการเงินอย่างธนาคาร Citibank ตลาดหลักทรัพย์ NASDAQ รวมไปถึงบริษัท VISA ก็ได้เข้าลงทุนในบริษัทบล็อกเชนชั้นนำอย่าง Chain.com เพื่อแนวทางรักษาตลาดเทคโนโลยีนี้เช่นกัน

**แนวคิด Blockchain** เริ่มกลับมาเป็นกระแสที่ต้องจับตามองอีกครั้ง พร้อมมีการพัฒนาใหม่ๆ ไปสู่การใช้งานที่มากกว่าการทำธุรกรรม Bitcoin ในอดีตที่ไม่ได้รับการยอมรับมากนัก ผสมรวมกับกระแสการเพิ่มขึ้นของอุปกรณ์ที่ใช้แนวคิด อินเทอร์เน็ต ออฟ ธิงส์ (Internet of Things) จำเป็นต้องมีการจัดการ ดูแลอย่างการรักษาความปลอดภัยระหว่างอุปกรณ์ต่างๆ และความจำเป็นที่จะต้องบันทึกฐานข้อมูลของการติดต่อต่างๆ เหล่านั้น ทำให้เทคโนโลยีอย่าง Blockchain ที่ให้ความสำคัญกับความเป็นส่วนตัวจะกลายมาเป็นตัวช่วยสำคัญของการใช้งานดังกล่าว โดยลดขั้นตอนระบบการทำงานให้เรียบง่ายขึ้น มีการยืดหยุ่นที่สูงขึ้น รวมทั้งการตอบสนองความต้องการของลูกค้าได้อย่างรวดเร็ว

แต่กระนั้นความสำเร็จของ Blockchain จะสามารถพลิกสถานะการให้บริการด้านการเงินโลกดิจิทัลได้หรือไม่ การหาพาร์ทเนอร์ที่มีประสิทธิภาพในการทำงานกับระบบความซับซ้อน และความหลากหลาย ในทุกระดับการใช้งานไม่ว่าเล็ก หรือใหญ่ เป็นหัวใจสำคัญของการจัดการกับปัญหานี้ได้ดีที่สุด ซึ่งถ้าย้อนกลับไปเมื่อ 5 ปีที่ผ่านมาไอเดียทางธุรกิจเหล่านี้ ต่างเคยถูกมองว่าเป็นเรื่องที่ไม่น่าจะเกิดขึ้นได้จริง หากแต่ปัจจุบันเรื่องเช่นนี้ได้กลายเป็นตัวกำหนดผู้ชนะในอนาคต ซึ่งทั้งหมดนี้สามารถเกิดขึ้นได้ด้วยการมองว่าซอฟต์แวร์คือตัวแปรสำคัญของการเปลี่ยนแปลงของโลกยุคใหม่นั้นเอง

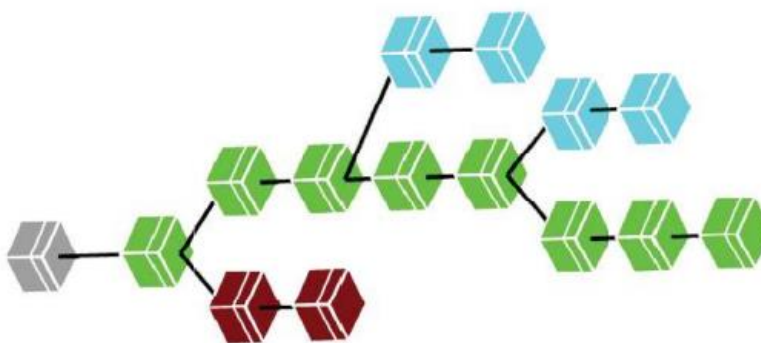
## หลักการทำงานของ Blockchain

**Blockchain** เป็นรูปแบบการเก็บข้อมูลแบบหนึ่งที่ทำให้ข้อมูล (Digital Transaction) ของแต่ละคนสามารถแลกเปลี่ยนข้อมูลกันได้โดยตรง และการเก็บข้อมูลไว้เป็นบล็อก (Block) แล้วทำแต่ละบล็อกมาเชื่อมโยงกันเป็นห่วงโซ่ (Chain) โดยที่การแลกเปลี่ยนข้อมูลกันสามารถรู้ว่าใครเป็นคนเข้าถึงข้อมูลและมีสิทธิ์ในการใช้ข้อมูลนั้นจริงๆ และเป็นเรื่องยากที่จะมีคนแอบมาเปลี่ยนแปลงข้อมูลเมื่อถูกเก็บลงใน Blockchain แล้ว โดยตรวจสอบความถูกต้องและรับประกันความปลอดภัยโดยวิทยาการเข้ารหัสลับ บล็อกแต่ละบล็อกจะมีค่าแฮชของบล็อกก่อนหน้าซึ่งทำหน้าที่ยืนยันความถูกต้องของบล็อกก่อนหน้า และยังมีการใส่ตารางเวลาของการทำธุรกรรม Blockchain ถูกออกแบบมาให้ทนทานต่อการเปลี่ยนข้อมูลที่บันทึกลงไปแล้ว คือจะเป็น

“บัญชีแยกประเภท (Ledger)” แบบกระจายและเปิด ที่สามารถบันทึกธุรกรรมระหว่างบุคคลได้อย่างมีประสิทธิภาพ ในรูปแบบที่ยืนยันได้และเก็บอย่างถาวร

Blockchain ใช้เครือข่ายเพียร์ทูเพียร์ (Peer to Peer) ซึ่งร่วมกันใช้โพรโทคอลเดียวกันเพื่อสื่อสารกันระหว่างโหนด และเพื่อยืนยันความถูกต้องของบล็อกใหม่ๆ เมื่อบันทึกแล้วข้อมูลในบล็อกใดบล็อกหนึ่ง จะไม่สามารถย้อนหลังโดยไม่เปลี่ยนข้อมูลในบล็อกต่อๆมาทั้งหมดด้วย จะทำได้ก็เมื่อได้รับความร่วมมือของโหนดในเครือข่าย

Blockchain ออกแบบมาตั้งแต่ต้นเพื่อความปลอดภัย (Secure by design) และเป็นตัวอย่างของระบบคอมพิวเตอร์แบบกระจายที่ทนต่อความผิดพลาด บกพร่อง แบบไบแซนไทน์ได้สูง



ภาพที่ 1 ภาพแสดงบล็อกเชนที่มีจุดต่อกันยาวสุดตั้งแต่ต้น โดยบล็อกเริ่มต้นที่สีเทา และบล็อกกำพรว้าเป็นสีน้ำตาลและฟ้า

## ประเภทของ Blockchain

การประยุกต์ใช้ Blockchain สามารถแบ่งเป็น 3 ประเภท ได้แก่

1. Public Blockchain เป็นบล็อกสาธารณะที่นำไปใช้จริงในระบบ Bitcoin หรือ Ethereum ซึ่งข้อมูลที่บันทึกเข้าไปจะถูกเปิดเผยต่อสาธารณะชน
  - a. ข้อดี คือ องค์กรไม่ต้องลงทุนค่าเครื่องมือและอุปกรณ์ราคาสูง
2. Private Blockchain เป็นบล็อกที่เราสร้างขึ้นมาเพื่อใช้งานภายในองค์กรเราเองได้ และภายในเครือข่ายเท่านั้นที่มีสิทธิ์เข้าถึงข้อมูลภายในบล็อก
  - a. ข้อดี คือ ข้อมูลไม่ถูกเผยแพร่สู่สาธารณะ และองค์กรสามารถปรับแต่งกฎเกณฑ์และเงื่อนไขต่างๆ ให้เหมาะสมกับองค์กรตัวเองได้
  - b. ข้อเสีย คือ องค์กรต้องลงทุนติดตั้งเครือข่ายโหนดเอง
3. Consortium Blockchain เป็นการรวมกันของ 2 แนวคิดแรกระหว่าง แบบสาธารณะ และ แบบส่วนตัว เข้าด้วยกันโดยเอาข้อดีของแต่ละแบบมาผสมกัน
  - a. ข้อดี คือ ทำให้องค์กรสามารถที่จะแลกเปลี่ยนข้อมูลกับองค์กรภายนอกได้ และข้อมูลบางส่วนที่ไม่ต้องการที่จะเผยแพร่ต่อสาธารณะสามารถที่จะเก็บไว้แบบส่วนตัวได้ ทำให้เกิดการร่วมทุนกับองค์กรอื่นๆ ได้
  - b. ข้อเสีย คือ เนื่องจากมีส่วนที่ต้องเกี่ยวข้องกับองค์กรอื่นทำให้บางส่วนไม่สามารถที่จะปรับปรุงได้ง่าย อาจต้องมีการลงมติความเห็นชอบของทั้งสององค์กร

รูปแบบการเข้ารหัสลับและถอดรหัสลับด้วย **ECDSA**

เทคโนโลยีการเข้ารหัสข้อมูล เป็นกระบวนการสำหรับการแปลงข้อมูลอิเล็กทรอนิกส์ธรรมดาให้อยู่ในรูปที่บุคคลทั่วไปไม่สามารถอ่านเข้าใจได้ การเข้ารหัสลับจะกระทำก่อนการจัดเก็บข้อมูลหรือก่อนส่งข้อมูล โดยการนำข้อมูลอิเล็กทรอนิกส์ธรรมดากับกุญแจ (Key) ซึ่งเป็นเลขซึ่งสุ่มมาผ่านกระบวนการวิทยาศาสตร์ ขั้นตอนที่กำลังจะเรียกว่า

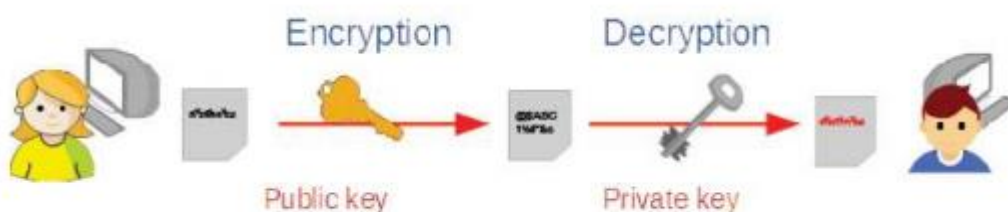
“การเข้ารหัสลับ” (ENCRYPTION) และต้องการอ่านข้อมูลจะต้องนำเอาข้อมูลที่เข้ารหัสและกุญแจมาผ่านกระบวนการทางคณิตศาสตร์ จะได้ผลลัพธ์ที่เป็นข้อมูลเดิม ขั้นตอนนี้จะเรียกว่า

“การถอดรหัส” (DECRYTION) ระบบการเข้ารหัสแบ่งตามวิธีการใช้กุญแจได้เป็น 2 วิธี คือการเข้ารหัสลับแบบกุญแจสมมาตร และ อสมมาตร



ภาพที่ 2 ภาพแสดงการเข้ารหัสลับแบบกุญแจสมมาตร

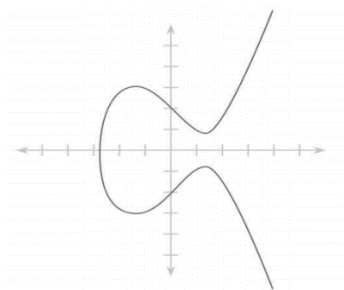
ระบบการเข้ารหัสลับแบบสมมาตร (Symmetric key cryptography) ด้วยกุญแจเดียว ทั้งผู้ส่งและผู้รับจะใช้กุญแจเดียวกันในการเข้ารหัสและถอดรหัส โดยวิธีการนี้ผู้ส่งและผู้รับจะต้องตกลงวิธีในการเข้ารหัสข้อมูลซึ่งก็คือกุญแจ



ภาพที่ 3 ภาพแสดงการเข้ารหัสลับแบบกุญแจอสมมาตร

ระบบการเข้ารหัสลับแบบกุญแจอสมมาตร (Asymmetric key cryptography) คือการเข้ารหัสลับที่ใช้กุญแจคู่ในการทำการเข้ารหัสและถอดรหัส โดยกุญแจจะประกอบไปด้วย กุญแจส่วนตัว (Private key) และกุญแจสาธารณะ (Public key) โดยหลักการทำงานคือ หากใช้กุญแจใดในการเข้ารหัส จะต้องใช้อีกกุญแจในการถอดรหัส และจะมีเฉพาะกุญแจคู่ของมันเท่านั้นที่จะสามารถถอดรหัสได้ ไม่สามารถนำกุญแจคู่อื่นมาถอดรหัสได้อย่างเด็ดขาด ในระบบ Ethereum ได้ใช้ ECDSA ในการเข้ารหัสและถอดรหัสบน Ethereum Smart contract

เพื่อใช้เป็น source ในการ random สำหรับ ECDSA (Elliptic Curve Digital Signature Algorithm) เป็นอัลกอริทึม ที่ Bitcoin กับ Ethereum ใช้ในการสร้างตัว Private Key, Public Key และ Address



ภาพที่ 4 ภาพแสดงตัวอย่างในการคำนวณ Elliptic Curve

## HASH

Hash คือการเข้ารหัสทางเดียว โดยจะสร้าง Digital Signature ของข้อมูล Digital ที่ไม่สามารถถอดรหัสกลับมาได้ และใช้เป็นตัวแทนของข้อมูลนั้นๆ โดยใช้หลักการของ Private Key และ Public Key

คุณสมบัติหลักๆของการ Hash คือ

1. ค่า Hash ของข้อมูลเดิมจะต้องเหมือนกันเสมอ ไม่ว่าจะ Hash กี่รอบก็จะได้ค่าเดิม
2. Collision-Free ค่า Hash ของข้อมูลที่ไม่เหมือนกันจะไม่มีทางเหมือนกัน
3. Hiding ไม่สามารถนำค่า Hash ที่ได้มาเพื่อถอดรหัสหาค่าข้อความเดิมได้
4. ค่า Hash จะมีความยาวเท่ากัน ไม่ว่าข้อความนั้นจะสั้นหรือยาว กล่าวคือเราจะได้ค่าจากการ Hash มีขนาดความยาวคงที่ที่เท่าเดิมเสมอ

Bitcoin ได้นำคุณสมบัติเหล่านี้มาใช้ในการตรวจสอบข้อมูลที่ถูกต้องของรายการ โดยสร้างเป็น Ledger Address ของแต่ละบัญชีเพื่อใช้แทนเลขบัญชีโดย Address สร้างจาก

1. Private key ซึ่งเป็น User/Password หรือเป็น Secret works ที่แต่ละคนจะกำหนดไว้ ซึ่งทุกคนต้องจำได้ ถ้าหากก็ไม่สามารถเข้าถึงบัญชีตัวเองได้
2. สร้าง Public key จาก Private key ขึ้นมา
3. เมื่อได้ Public key ก็จะทำการคำนวณหาค่า Hash (SHA-256) เพื่อให้ค่าที่มีความยาว 33-34 ไบต์ (Base58 string) และเอามาใช้แทนเลขบัญชี



## ความเป็นส่วนตัว (Privacy) บนเทคโนโลยีบล็อกเชน (Blockchain)

หนึ่งในคุณสมบัติสำคัญของบล็อกเชนคือ 'ความโปร่งใส' เนื่องจากธุรกรรมใดๆ ก็ตามที่ถูกกระทำผ่าน บล็อกเชนข้อมูลเหล่านั้นจะถูกเปิดเผยต่อสาธารณะ เพื่อให้มีการตรวจสอบและยืนยันความถูกต้องจากเครือข่าย ได้ ดังนั้นไม่ว่าใครก็ตาม ที่อยู่ภายในเครือข่ายระบบก็จะสามารถมองเห็นการทำธุรกรรมต่างๆ ที่เกิดขึ้นได้ ไม่ว่าจะเป็น เกี่ยวข้องหรือไม่เกี่ยวข้องกับข้อมูลนั้นก็ตาม ด้วยเหตุนี้เองจึงทำให้ 'ความเป็นส่วนตัว' ของผู้ใช้งานเทคโนโลยี บล็อกเชนหายไปอย่างสิ้นเชิง

ถึงแม้ว่าในปัจจุบันจะมีคริปโทเคอร์เรนซีบางสกุลที่มีวัตถุประสงค์ในการรักษาความเป็นส่วนตัวของผู้ใช้งาน โดยพัฒนาโปรโตคอล (Protocol) ที่มีคุณลักษณะพิเศษในการรักษาความเป็นส่วนตัวระดับสูงในการทำ ธุรกรรมบนบล็อกเชน อาทิ Zcoin, Zcash หรือ Monero ที่เน้นการรักษาความลับในการทำธุรกรรมของผู้ใช้งาน ให้สามารถปกปิดเส้นทางหรือที่มาที่ไปของธุรกรรม ทำให้ไม่สามารถตามรอยได้ ด้วยเหตุนี้เหรียญเหล่านี้จึงถูก มองว่าอาจสามารถใช้เป็นช่องทางในการหลบเลี่ยงการตรวจสอบเส้นทางการเงินหากมีการใช้ผิดวัตถุประสงค์

จากที่กล่าวไปข้างต้น เหมือนจะเข้าทางสำนักที่ว่า 'ได้อย่างเสียอย่าง' ที่ทำให้ผู้ใช้งานต้องเลือกระหว่าง 'ความเป็นส่วนตัว' หรือ 'ความโปร่งใส' แต่เมื่อเร็วๆ นี้ ในประเทศไทยได้มีผู้พัฒนา Network เพื่อตอบโจทย์ทั้ง เรื่อง 'ความโปร่งใส' และ 'ความเป็นส่วนตัว' เข้าไว้ด้วยกัน หรือเรียกว่า Balance Overall หรือ BO Network เป็น เครือข่ายที่เชื่อมต่อสินทรัพย์ดิจิทัลทุกประเภทไม่ว่าจะเป็น คริปโทเคอร์เรนซี หรือดิจิทัลโทเคนมีคุณสมบัติ สำคัญคือ ทุกคนที่ใช้ BO Network นี้ สามารถทำธุรกรรมที่มีความเป็นส่วนตัวได้ โดยยังใช้เทคโนโลยีบล็อก เชนเพื่อรักษาคุณสมบัติในความโปร่งใส ตรวจสอบได้อยู่ โดยข้อมูลธุรกรรมต่างๆที่เกิดขึ้นจะถูกกำหนดการ เข้าถึงเฉพาะร้านค้า และผู้ซื้อสินค้าเท่านั้น

เปรียบเทียบกับที่เราใช้เงินบาทเช่นธนบัตร 100 บาทเพื่อซื้อของกับร้านค้า จะพบว่าการทำธุรกรรม ดังกล่าว ร้านค้าและผู้ซื้อสินค้าเท่านั้นที่ทราบว่ามีการทำธุรกรรมระหว่างกัน เมื่อยุคสมัยเปลี่ยนไปเทคโนโลยีมี ความเจริญมากขึ้น การใช้โทรศัพท์มือถือเพื่อทำการโอนเงินระหว่างผู้ซื้อและร้านค้าเป็นเรื่องสะดวกสบายมาก ยิ่งขึ้นส่งผลให้แอปพลิเคชันอย่าง SCB Easy KPlus หรือ ICBC Mobile Bank เป็นที่นิยมอย่างแพร่หลาย จาก ความสะดวกสบายดังกล่าว พบว่าข้อมูลธุรกรรมนั้น ๆ ไม่ได้รับรู้แค่ผู้ซื้อและผู้ขายเหมือนการใช้ธนบัตร 100 บาทอีกต่อไปแล้ว เพราะข้อมูลธุรกรรมดังกล่าว ธนาคารต้นทาง และธนาคารปลายทางสามารถเข้าถึงข้อมูล ดังกล่าวได้ด้วย

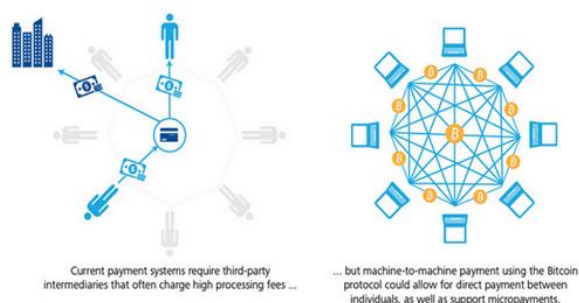
การเกิดขึ้นของเทคโนโลยีบล็อกเชนเมื่อไม่นานมานี้ทำทุกคนต่างให้ความสนใจ มีการนำไปใช้เพื่อเป็น เทคโนโลยีสำหรับการโอนเงินที่ไม่ใช่แอปพลิเคชันดิจิทัลแบงก์กิ้ง ตัวอย่างเช่น Bitcoin ที่ทุกคนต่างเคยได้ยิน ชื่อ และมีการใช้งานอย่างแพร่หลายมากขึ้นทุก ๆ ปี แต่สิ่งหนึ่งที่ทุกคนต่างลืมไปก็คือ การทำธุรกรรมดังกล่าว

ไม่ใช่เพียงแค่ธนาคารเท่านั้นที่เห็น แต่กลับเป็นว่าทุก ๆ คนที่ไม่ได้มีส่วนเกี่ยวข้องกับธุรกรรมดังกล่าวสามารถเห็นได้ด้วย

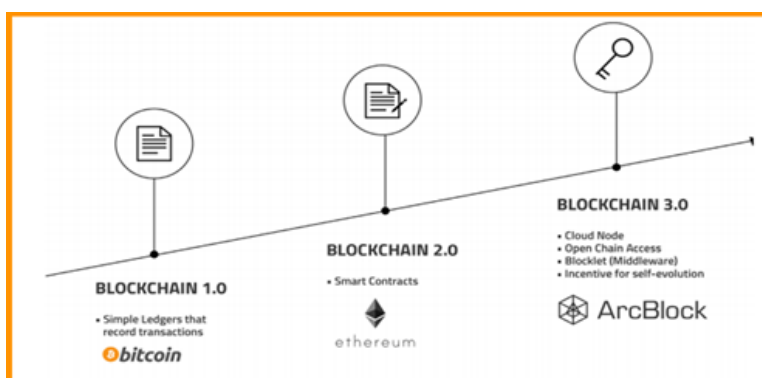
นั่นจึงเป็นที่มาของ Balance Overall (BO) Network เครือข่ายที่เชื่อมสินทรัพย์ดิจิทัลทุกประเภทในโลกนี้ได้ ไม่ว่าจะเป็น คริปโทเคอร์เรนซ์ดิจิทัลโทเคนที่ทำงานแทนธนบัตรหรือเงินสดที่ออกโดยธนาคารในทุกๆ ประเทศ ให้มีความสามารถในการทำธุรกรรมที่มีความเป็นส่วนตัวสำหรับร้านค้าและผู้ซื้อสินค้าเท่านั้น ที่จะเข้าถึงข้อมูลธุรกรรมได้ เสมือนการใช้ธนบัตรในรูปแบบดิจิทัลอย่างแท้จริง

## พัฒนาการของ Blockchain

พัฒนาการของ Blockchain โดย Blockchain เป็นเทคโนโลยีที่ช่วยนำมาซึ่งความปลอดภัย น่าเชื่อถือ โดยไม่ต้องอาศัยคนกลาง และเป็น platform ในการทำธุรกรรมแบบ peer-to-peer ที่มีการบันทึกข้อมูลรายการธุรกรรมทั้งหมดแบบกระจายศูนย์ (Decentralize)



ภาพที่ 5 ภาพด้านซ้ายเป็นระบบ Payment ในปัจจุบันที่ต้องผ่านคนกลาง ภาพด้านขวาเป็นการทำธุรกรรมแบบ peer-to-peer ที่มีการบันทึกข้อมูลรายการธุรกรรมทั้งหมดแบบกระจายศูนย์ (Decentralize)



ภาพที่ 6 พัฒนาการของ Blockchain

(จากรูปภาพที่ 6) ในยุคแรก หรือ Blockchain 1.0 เริ่มเมื่อปี ค.ศ. 2008 ได้ถูกพัฒนาเป็นครั้งแรกในภาคการเงิน โดย ประกอบด้วยสกุลเงินแบบเสมือน (เงินดิจิทัล) เช่น Bitcoin ซึ่งสามารถใช้แทนสกุลเงินจริงได้ เช่น ยูโร หรือ ดอลลาร์ และในวันนี้ Bitcoin ถูกนำมาใช้ในแอปพลิเคชันของ Blockchain และที่เป็นที่รู้จักกันดีที่สุดของคนทั่วไป และกำลังจะถูกนำมาใช้มากขึ้น อย่างไรก็ตามแม้ว่าในความเป็นจริงจะมีการใช้สกุลเงินมากมาย และด้วยปริมาณการซื้อขายที่สูงขึ้น แต่ส่วนแบ่งตลาดของ Bitcoin ในตลาดแลกเปลี่ยนเงินตราต่างประเทศยังคงน้อยมาก ซึ่งปัจจุบันยังไม่มีข้อบ่งชี้ว่า Bitcoin อาจจะมีสำคัญใกล้เคียงกับสกุลเงินต่างๆ ได้

ต่อมาการพัฒนา Blockchain ในระยะต่อมา Blockchain 2.0 เมื่อปี ค.ศ. 2014 ได้กำเนิดสกุลเงินดิจิทัล หรือ Cryptocurrency ที่ชื่อว่า Ethereum ขึ้น ที่ใช้เทคโนโลยี Blockchain ที่พัฒนาขึ้น โดย Vitalik Buterin โดยในยุคนี้เป็นยุคที่ Blockchain พัฒนาความสามารถในการเขียนโปรแกรมหรือที่เรียกกันว่า Smart Contract บน Blockchain โดย smart contract หมายถึง กระบวนการทางดิจิทัล ที่กำหนดขั้นตอนการทำธุรกรรมโดยอัตโนมัติไว้ล่วงหน้า โดยไม่ต้องอาศัยตัวกลาง อย่างเช่น ธนาคาร ซึ่งการสร้าง smart contract ที่เป็นระบบอัตโนมัติอย่างเต็มรูปแบบ โดยคู่สัญญาทั้งสองฝ่ายจะมีการตกลงกันก่อนหน้านั้น ถึงขั้นตอนกลไกในการทำรายการธุรกรรมดังกล่าว ซึ่งการพัฒนาสิ่งส่งผลกระทบต่อรูปแบบธุรกิจแบบดั้งเดิมของธนาคาร บริษัทและนักพัฒนา อาจตัดสินใจสร้างแอปพลิเคชันของตนบน Blockchain สาธารณะ หรือ Blockchain ส่วนตัว โดยใน Blockchain แบบสาธารณะนั้น ระบบจะไม่มี การเปิดเผยตัวตนของผู้เข้าร่วม ตัวอย่างของสกุลเงินที่ใช้ใน Blockchain ได้แก่ Bitcoin และ Ethereum เป็นต้น นอกจากนี้ในระบบ Blockchain แบบส่วนตัวนั้น ผู้เข้าร่วม Blockchain ทั้งหมดจะเป็นที่รู้จัก และต้องระบุตัวตนก่อนที่จะได้รับสิทธิ์ให้เข้าใช้ระบบ โดยข้อดีบางประการของ Blockchain แบบส่วนตัว คือช่วยให้มีโครงสร้างในการกำกับดูแลง่ายขึ้น และสามารถใช้งานได้โดยมีค่าใช้จ่ายที่ต่ำกว่า เมื่อเทียบกับแอปพลิเคชัน Blockchain สาธารณะ ดังนั้นธนาคารและผู้ให้บริการชำระเงิน จำเป็นจะต้องใช้ Blockchain แบบส่วนตัว สำหรับรูปแบบทางธุรกิจที่มีอยู่ในปัจจุบัน เพื่อให้สามารถรักษาระดับในการควบคุมความปลอดภัยได้อย่างมีประสิทธิภาพ

ต่อมาการพัฒนาเทคโนโลยี Blockchain ในระยะถัดมา (Blockchain 3.0) ในปี ค.ศ. 2017 ซึ่งเป็น ยุคของ Dapp หรือ Decentralized application โดยมีแนวคิดเกี่ยวกับ smart contract เพื่อสร้างกระบวนการแบบกระจายศูนย์ที่เป็นอิสระ ที่ต้องมีการกำหนดกฎการทำธุรกรรมของกลุ่มกันเองและดำเนินการด้วยความเป็นอิสระ ในรูปแบบธุรกรรมอัตโนมัติ ซึ่งถือเป็นการเปิดประตูไปสู่อุตสาหกรรมอื่นๆ อีกมากมาย โดยผู้ประกอบการสามารถนำ smart contract มาสร้าง Application ที่แก้ปัญหาในชีวิตจริงและ disrupt ธุรกิจโมเดลเดิมๆ

## ทำความเข้าใจกับ Ethereum และ smart contract

**Ethereum** เป็นหนึ่งในสกุลเงินดิจิทัล ได้รับการพัฒนาจากเด็กหนุ่มชาวรัสเซีย นามว่า Vitalik Buterin ซึ่งเขาอยู่ในทีมพัฒนาเหรียญบิตคอยน์มาก่อนและการทำงานที่เขาต้องการที่จะสร้างเหรียญสกุลนี้ขึ้นมา ก็เพื่อต้องการให้ใช้งานได้เหมือนกับเหรียญบิตคอยน์แต่เพิ่มความสามารถของเหรียญให้มากยิ่งขึ้นเพื่อจะได้อตอบสนองต่อความต้องการของผู้ใช้งานสกุลเงินนี้จึงไม่ได้จำกัดแค่เพียงการใช้งานด้านการงานแต่ยังสามารถใช้ในการดำเนินธุรกิจต่างๆได้ด้วยอันที่จริงแล้ว Ethereum และบิตคอยน์ไม่ได้ต่างกันเลย เพราะว่าเป็นเงินสกุลดิจิทัลเหมือนกัน และชุด ข้อขายเก็งกำไรได้เหมือนกัน และในบางประเทศโดยเฉพาะประเทศญี่ปุ่นและประเทศสวิสเซอร์แลนด์ก็ให้การยอมรับในการซื้อสินค้าและบริการได้ แต่บิตคอยน์ก็มีข้อแตกต่างอยู่บ้างตรงที่เป็นแค่สกุลเงินจะพัฒนาหรือทำอะไรมาไม่ได้ แต่สำหรับสกุลเงิน Ethereum นั้น เปิดให้ทุกคนเข้ามาเขียนข้อมูลบนสกุลเงินเพื่อร่วมกันพัฒนาได้เพราะออกแบบมาให้เป็นระบบ Open Source ซึ่งถือเป็นข้อดีอย่างมากเพราะมันทำให้ทุกคนเข้าถึงสกุลเงินนี้ได้ และยังสามารถพัฒนาให้ตอบโต้กับคนที่ให้บริการอีกด้วย และดูเหมือนว่าความนิยมของ Ethereum จะมีมากขึ้นเรื่อยๆ พร้อมๆกับการเติบโตของสกุลเงินอื่นๆ ที่คุณสามารถเลือกได้เองว่าต้องการลงทุนแบบไหนอย่างไร และจะอย่างไรบ้างกับสกุลเงินนี้ อย่างเช่น การชำระค่าใช้จ่าย ธุรกิจการเช่ารถหรือรถรับจ้างที่มีการใช้ระบบ Smart Contract ที่มีความสามารถเฉพาะตัวของ Ethereum โดยที่จะคล้ายคลึงกับ Uber และ Grab Bike หรือ Grab Taxi แต่จะแตกต่างกันตรงที่ว่าชำระค่าบริการผ่านแพลตฟอร์ม Ethereum นั้นไม่จำเป็นต้องผ่านคนกลาง ดังนั้นจึงทำให้นักลงทุนหลายคนสนใจในสกุลเงิน Ethereum นี้กันมากแต่อย่างไรก็ตาม คุณต้องทำความเข้าใจว่าการลงทุนทุกอย่างมีความเสี่ยงจึงต้องระมัดระวังในเรื่องของการลงทุนให้มากเพราะถึงแม้สิ่งเหล่านี้จะถูกคิดค้นขึ้นมา แต่ในความเป็นจริงแล้วมันยังเพิ่งถูกเริ่มทดสอบใช้และยังไม่ได้ถูกเอามาใช้ในชีวิตจริง

## Ethereum Messages และ Transactions

ในแต่ละโหนดของ Ethereum จะประกอบด้วยข้อมูลบัญชี (Account) เพื่อใช้ระบุตัวตน สำหรับการทำรายการต่างๆในระบบ โดยรายการต่างๆที่เกิดขึ้นในระบบจะเรียกว่า Transaction หรือ Message

**Transaction** หมายถึงชุดข้อมูลที่ถูกทำ digitally sign ซึ่งบรรจุข้อความ (Message) ที่จะส่ง หากันไปมาระหว่าง account หนึ่งถึง account หนึ่ง โดยที่ภายใน Transaction นั้น ประกอบด้วย

1. ที่อยู่ของผู้รับ Message โดยจะเป็นเลขฐาน 16 ขนาด 20 ไบท์
2. Digital signature ที่ผู้ส่งทำการ Digitally sign Message อันนี้มา (ข้อมูลที่ถูกเข้ารหัสลับ)
3. เงินที่ถูกส่งจากผู้ส่ง
4. ข้อมูลอื่นๆ ซึ่งสามารถเป็นข้อมูลอะไรก็ได้ทั้งตัวเลข ตัวอักษร รวมไปถึงไฟล์ต่างๆ โดยจะอยู่ในรูปแบบเลขฐาน 16
5. STARTGAS ค่าตัวเลขสูงสุดของ Step การประมวลผล Transaction ที่จะให้ miner ทำการประมวลผลซึ่งมีขึ้นเพื่อป้องกันการเกิดปัญหา miner ในการทำงานใน Transaction แบบไม่รู้จบ
6. GASPRICE ค่าธรรมเนียมที่ผู้ส่งจะต้องจ่ายเพื่อให้ miner ทำงานใน transaction นี้

**Message** คือข้อความที่ส่งไปมาหากันระหว่าง Contract โดยที่จะไม่ถูกนำเข้าไปในบล็อก เช่นและจะอยู่แค่เฉพาะส่วนตอน miner กำลังประมวลผลคำสั่งของ contract เท่านั้น โดยภายใน ของ message จะประกอบด้วย

1. ที่อยู่ของผู้ส่ง Message โดยเป็นเลขฐาน 16 ขนาด 20 ไบท์
2. ที่อยู่ของผู้รับ Message โดยเป็นเลขฐาน 16 ขนาด 20 ไบท์
3. จำนวนเงินที่แนบมาใน Message
4. ข้อมูลอื่นๆ ซึ่งสามารถเป็นข้อมูลอะไรก็ได้ทั้งตัวเลข ตัวอักษร รวมไปถึงไฟล์ต่างๆ โดยจะอยู่ในรูปแบบเลขฐาน 16
5. STARTGAS ค่าตัวเลขสูงสุดของ Step การประมวลผล Transaction ที่จะให้ miner ทำการประมวลผลซึ่งมีขึ้นเพื่อป้องกันการเกิดปัญหา miner ในการทำงานใน Transaction แบบไม่รู้จบเป็นรูปไปเรื่อยในระบบ

โดยพื้นฐานแล้ว Message จะคล้ายกันกับ Transaction ต่างกันแค่ Message จะสร้างมาจาก Contract ในขณะที่ Transaction จะสร้างจากคน ซึ่ง Message นั้นจะถูกสร้างตอนที่ Contract มีการเรียกใช้คำสั่ง CALL

## อะไรคือ Smart Contract ?

**Smart Contract** มีความหมายโดยง่ายแบบตรงตัวก็คือ “สัญญา อัจริยะ” ซึ่งเข้ามาช่วยให้คุณสามารถแลกเปลี่ยน เงิน หรือสิ่งของอะไรก็ได้ที่มีมูลค่าได้อย่างโปร่งใสปราศจากความขัดแย้งและหลีกเลี่ยงจากพ่อค้าคนกลางซึ่งโดยปกติสัญญาได้ระบุไว้อย่างชัดเจนว่า เงินทุนต้องถึงเท่าไรในระยะเวลาที่กำหนด และระยะเวลาในการพัฒนาถึงเมื่อไหร่ เป็นต้น และเมื่อเงินทุนถึงตามเป้าที่ตั้งไว้ก่อนกำหนด เงินทุนก็จะถูกโอนไปยังทีมพัฒนาโดยอัตโนมัติ และเมื่อโครงการพัฒนาได้สำเร็จสินค้าก็จะถูกส่งไปยังผู้ที่สนับสนุน แต่ถ้าหากโครงการไม่สำเร็จ เงินทุนก็จะถูกโอนกลับไปยังผู้สนับสนุนโดยอัตโนมัติด้วยเช่นกันนั่นหมายความว่า Smart Contract เป็นชิ้นส่วนของซอฟต์แวร์ที่จัดเก็บกฎสำหรับการเจรจาเงื่อนไขของข้อตกลงโดยอัตโนมัติ และมีการยืนยันความสำเร็จและจากนั้นดำเนินการตามเงื่อนไขที่ตกลงกันไว้ ทั้งหมดนี้จะอยู่บนระบบ Blockchain อีกทีหนึ่ง

**Smart Contract** คือโปรแกรมคอมพิวเตอร์ขนาดเล็กซึ่งถูกเก็บไว้ในรูปของบล็อกเชนอีเธอร์ียม ตัวสมาร์ทคอนแทรคสามารถใช้งานได้โดยใส่เหรียญอีเธอร์ียมเข้าไปในตัวสัญญานั้นๆ นอกเหนือจากนั้น Smart Contract จะระบุกฎระเบียบระหว่างผู้ซื้อและผู้ขายไว้ซึ่งมันจะช่วยอำนวยความสะดวกในเรื่องของการแลกเปลี่ยนเอกสาร, หุ่นในบริษัท, เงิน, สินทรัพย์ และอื่นๆอีกมากมายที่มีมูลค่าในตัวมันเอง โดยสมาร์ทคอนแทรคมีจุดประสงค์หลักคือ ตรวจสอบ, ยืนยัน, บังคับใช้หรือเซ็นสัญญาและข้อตกลงต่างๆผ่านระบบดิจิทัล

Smart Contract แตกต่างจากสัญญาทั่วไปตรงที่สมาร์ทคอนแทรคสามารถดำเนินการหรือยืนยันข้อตกลงต่างๆได้อย่างอัตโนมัติโดยไม่ต้องผ่านตัวกลาง อาทิเช่น ธนาคาร, รัฐบาล, โบรกเกอร์, ตัวแทนหรือทนาย

ซึ่งตามจริงแล้ว ตัวบล็อกเชนของบิตคอยน์ก็สามารถสร้างสมาร์ทคอนแทรคในนั้นได้ แต่ข้อเสียหลักๆของมันก็คือโครงสร้างภาษาของโปรแกรมคอมพิวเตอร์ที่มันซับซ้อนเกินกว่าที่จะนำไปพัฒนาระบบต่างๆได้ ซึ่งจะแตกต่างจากบล็อกเชนของอีเธอร์ียมที่เป็นมิตรกับนักเขียนโปรแกรมมากกว่าเนื่องด้วยโครงสร้างของระบบที่สามารถทำงานได้โดยไม่ติดขัดเรื่องภาษาโปรแกรม

### ปัจจุบันสามารถแบ่ง Smart contract ได้ 2 ประเภท คือ

1. Smart Contract Code คือรูปแบบที่คุ้นเคยมากที่สุด เพราะคือระบบที่นักพัฒนาโทเคนดิจิทัลนำมาใช้อำนวยความสะดวกในการดำเนินธุรกรรมบนเครือข่าย โดยมีคุณลักษณะสำคัญคือ จะต้องทำงานโดยอัตโนมัติ (execute automatically) ติดตามได้ (trackable) และไม่สามารถ เปลี่ยนแปลงและแก้ไขไม่ได้ (inalterable and irreversible) ปัจจุบันแพลตฟอร์ม Smart Contract Code ที่ได้รับความนิยมคือ อีเธอร์เรียม (Ethereum) นีโอ (NEO) และอีโอเอส (EOS)

2. Smart Legal Contract คือการนำโค้ด Smart Contract มาใช้เพิ่มประสิทธิภาพการบังคับใช้สัญญาแบบดั้งเดิมที่เป็นกระดาษ ซึ่งจะช่วยลดความซับซ้อนของกระบวนการต่างๆ ที่เกี่ยวข้อง แต่การ

ประยุกต์ใช้งานลักษณะดังกล่าวยังมีข้อจำกัด คือการยอมรับจากสถาบันและหน่วยงานทาง กฎหมาย ตลอดจน สังคมในภาพรวม

Smart Contract มีศักยภาพในการนำไปประยุกต์ใช้อำนวยความสะดวกในการดำเนินธุรกรรมให้เกิดขึ้น อัตโนมัติ โดยไม่ต้องอาศัยตัวกลาง จึงสามารถนำไปใช้ในภาคธุรกิจต่างๆ ได้หลากหลาย เพราะคู่สัญญาสามารถ มั่นใจได้ว่าอีกฝ่ายจะต้องรับผิดชอบต่อเงื่อนไขที่สำคัญ การที่ไม่สามารถแก้ไขหรือปรับเปลี่ยนสัญญาเมื่อเข้าสู่ ระบบบล็อกเชนได้ คือการประกันไว้ในระดับหนึ่งว่าอีกฝ่ายจะไม่สามารถแก้ไขสัญญาเพื่อประโยชน์ส่วนตัว Smart Contract จึงเหมาะสมกับภาคส่วนที่มีความอ่อนไหวและมีผลกระทบในวงกว้าง อาทิ ภาคการเงิน และ การบริหารงานภาครัฐ

## สมาร์ทคอนแทรคทำงานอย่างไร ?

### · การสร้างข้อตกลง

- ข้อตกลงระหว่างผู้ซื้อและผู้ขายจะถูกแปลงเป็นรหัสคอมพิวเตอร์ จากนั้นการทำธุรกรรมต่างๆ ที่เกิดขึ้นจะถูกบันทึกโดยอัตโนมัติในบล็อกเชนของอีเธอเรียม สมาร์ทคอนแทรคแต่ละอันจะมีหมายเลข ที่อยู่เป็นของตัวเองและเมื่อใดก็ตามที่สมาร์ทคอนแทรคถูกบันทึกในบล็อกเชนของอีเธอเรียมใครก็ตามที่มีที่อยู่ของตัวสมาร์ทคอนแทรคนั้นๆจะสามารถเข้าถึงสมาร์ทคอนแทรคได้

### · Triggering Events

- สมาร์ทคอนแทรคจำเป็นที่จะระบุถึงเหตุการณ์/จุดประสงค์พร้อมด้วยวันหมดอายุของสัญญา เพื่อให้ตัวสมาร์ทคอนแทรคทำงานได้ด้วยตัวมันเองโดยพิจารณาจากข้อตกลงที่ถูกแปลงเป็นรหัส ซึ่ง รหัสเหล่านี้จะระบุขั้นตอนต่างๆ โดยอาศัยหลักเหตุและผล เราสามารถอธิบายหลักเหตุและผลได้ว่า ถ้า คำสั่งชุดหนึ่งถูกส่งออกมาก็จะให้ผลในรูปแบบรูปแบบหนึ่ง โดยสมาร์ทคอนแทรคก็จะทำงานไปเรื่อยๆ จนกว่าทั้งผู้ซื้อและผู้ขายจะยุติสัญญา

### · การยุติข้อตกลง

- เมื่อสมาร์ทคอนแทรคถูกสร้างมาแล้ว ผู้ซื้อและผู้ขายจำเป็นที่จะบรรลุจุดประสงค์หรือเหตุการณ์ ต่างๆตามที่ได้ตกลงกันไว้ตอนแรก ถ้าหากฝ่ายใดฝ่ายหนึ่งไม่ได้ทำตามทีระบุไว้ในสัญญาภายใน ระยะเวลาที่ตกลงกันไว้ บล็อกเชนจะคืนเงิน ไปให้อีกฝ่ายหนึ่ง

## เครื่องมือต่าง ๆ สำหรับการเริ่มพัฒนา

- Remix Ethereum IDE Online เป็นเครื่องมือใช้เขียน Code, Compile, Deploy เป็นแบบออนไลน์สามารถ  
ใช้เขียนทดลอง รวมไปถึง Run ให้ทำงานจริงได้เลย มีความสะดวกในการใช้งาน

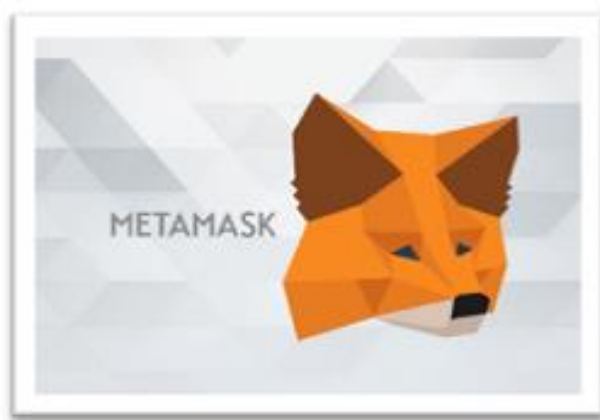


ภาพที่ 7 หน้าตาของ Remix Ide

- MetaMask (Browser Extension) ใช้เป็น Program ที่ใช้สร้างกระเป๋าเงินออนไลน์ เป็นส่วนขยายในเว็บ  
เบราว์เซอร์ Chrome, Firefox, Opera ใช้งานได้ง่ายและมีเซฟเวอร์ทดลองให้นักพัฒนาได้ Test ก่อนนำไปใช้งาน  
จริง

ในการใช้บล็อกเชนคุณต้องติดตั้งเบราว์เซอร์แอปพลิเคชันแบบกระจาย (dApp) สำหรับอุปกรณ์พกพา หนึ่งใน  
เบราว์เซอร์ dApp ที่ได้รับความนิยมมากที่สุดคือ Metamask

### การติดตั้ง Metamask



ภาพที่ 8 Logo Metamask

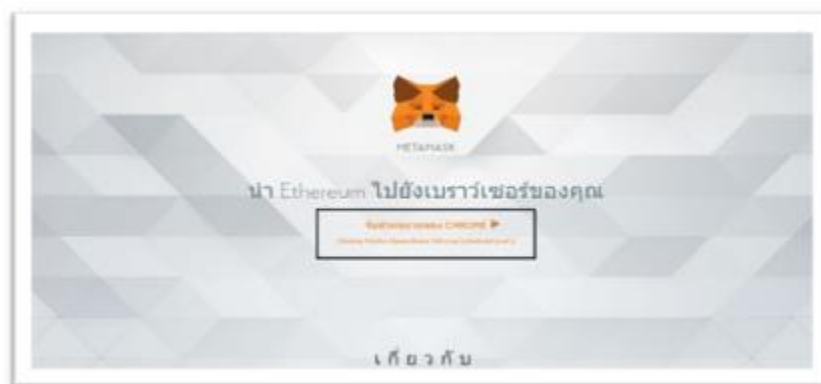


ขั้นตอนที่ 1 ไปที่เว็บไซต์ Metamask



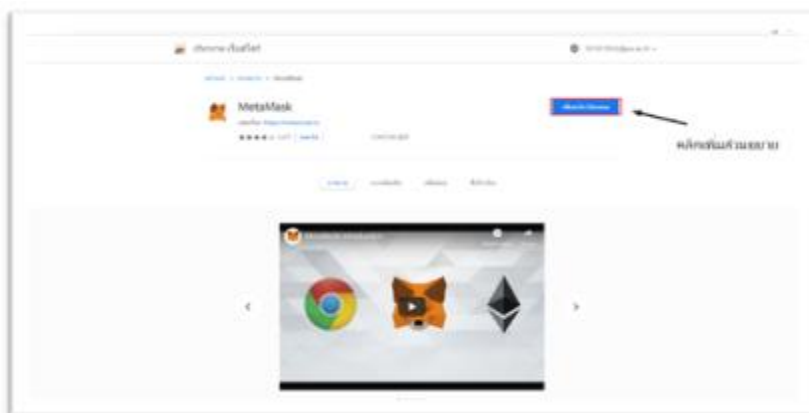
ภาพที่ 9 หน้าเว็บ Metamask

ขั้นตอนที่ 2 คลิก “รับส่วนขยายของ Chrome” เพื่อติดตั้ง Metamask



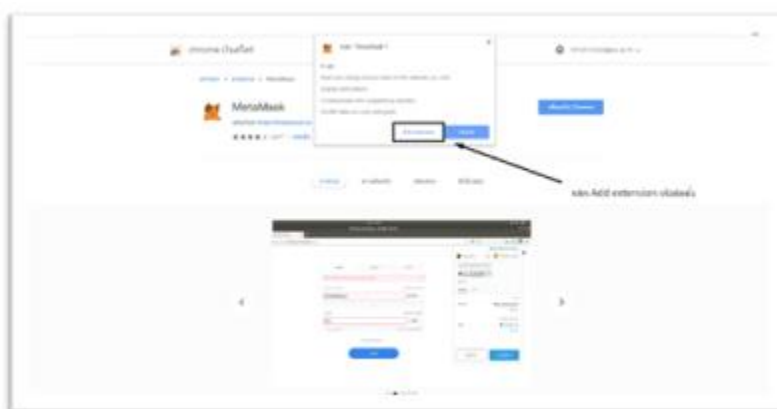
ภาพที่ 10 คลิกรับส่วนขยาย

ขั้นตอนที่ 3 คลิก “เพิ่มลงใน Chrome” ที่มุมขวาบน

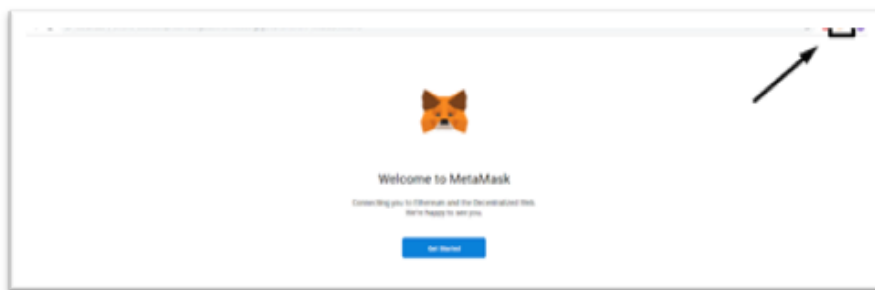


ภาพที่ 11 เพิ่ม Metamask ใน chrome

ขั้นตอนที่ 4 คลิก “เพิ่มส่วนขยาย” เพื่อทำการติดตั้งให้เสร็จ



ภาพที่ 12 เพิ่ม Add extension Metamask ใน chrome



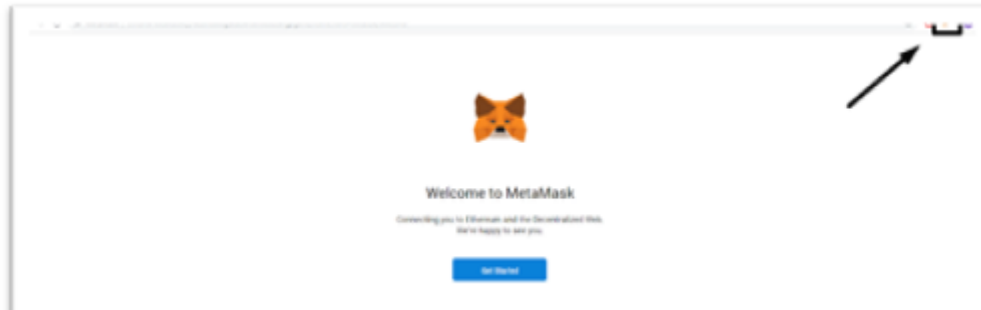
ภาพที่ 13 สังเกตมุมขวาบนเมื่อติดตั้งสำเร็จ

คุณจะรู้ว่า Metamask ได้รับการติดตั้งสำเร็จเมื่อเห็นโลโก้จิ้งจอกที่มุมบนขวาของเบราว์เซอร์ของคุณ

### การใช้งาน Metamask

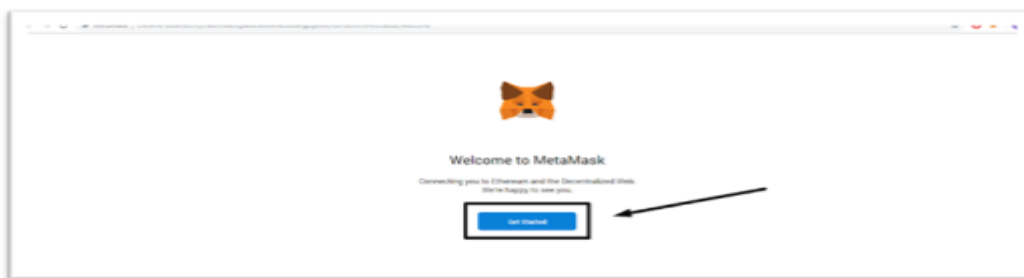
สิ่งแรกที่ต้องทำในการใช้ Metamask ก็คือการสร้าง บัญชีผู้ใช้ หรือ Wallet เพื่อใช้ในการเก็บ Token ของ Ethereum

**ขั้นตอนที่ 1** คลิกที่โลโก้ Metamask ที่มุมบนขวาของเบราว์เซอร์ที่ติดตั้ง Metamask



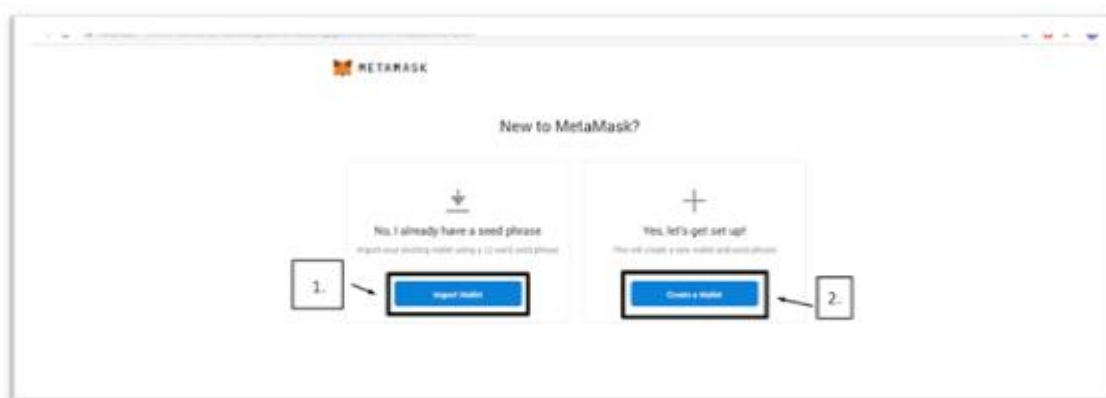
ภาพที่ 14 คลิกเข้า Metamask

ขั้นตอนที่ 2 คลิก Get start เพื่อเริ่มการสมัคร บัญชี



ภาพที่ 15 Get Started Metamask

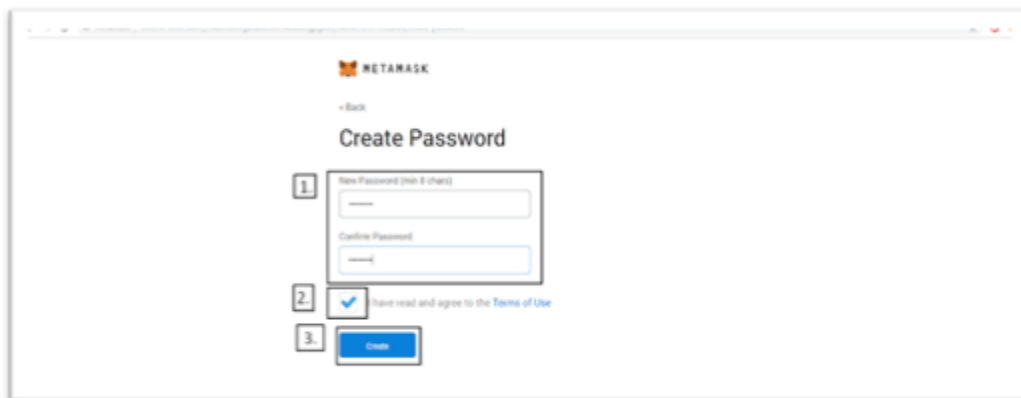
ขั้นตอนที่ 3 เลือก Import Wallet หรือ Create Wallet ตามความต้องการ



ภาพที่ 16 สร้างหรือเข้าสู่ระบบ

1. Import Wallet เลือกเพื่อเข้าสู่ระบบหากท่านมี Wallet ของ Metamask อยู่แล้ว
2. Create Wallet เลือกเพื่อสมัครสมาชิกเพื่อสร้าง Wallet ของตัวเอง

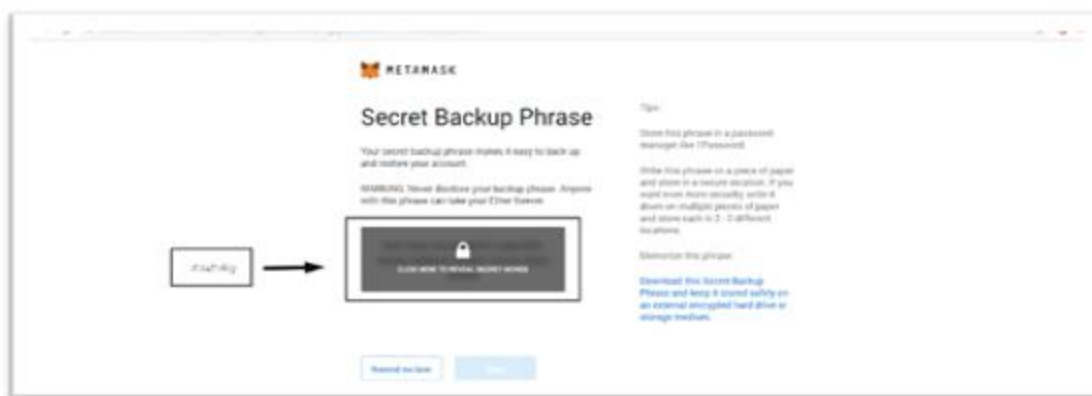
#### ขั้นตอนที่ 4 สร้างรหัสผ่านของ Wallet ของคุณ



ภาพที่ 17 สร้างรหัสผ่าน Metamask

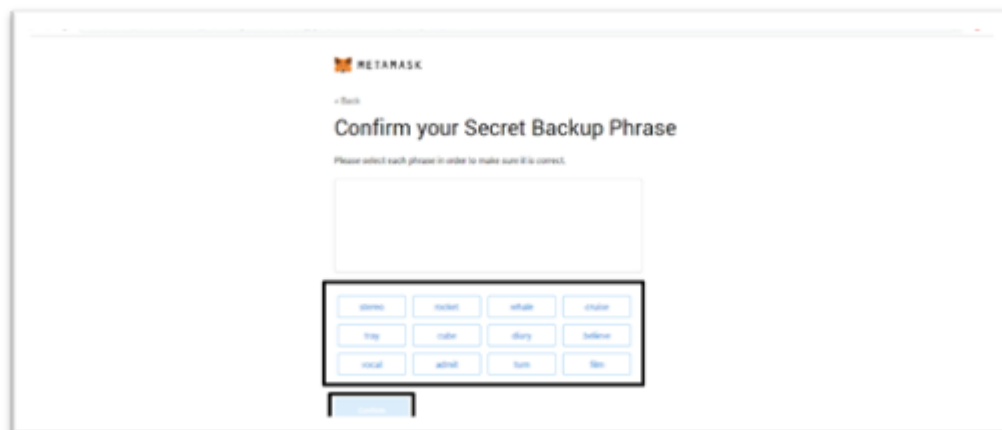
1. ตั้งรหัสให้เหมือนกันทั้ง 2 ช่อง
2. เลือกยอมรับข้อตกลง
3. คลิกสร้างเพื่อให้ Metamask สร้าง Wallet

ขั้นตอนที่ 5. ในขั้นตอนนี้คือขั้นตอนการสร้างบัญชี คือคลิกที่รูปแม่กุญแจจะได้ชุดคำ 12 คำซึ่งลำดับของคำเหล่านั้นคือ ID ของท่านที่ต้องจดบันทึกไว้เพื่อใช้ยืนยันในหน้าถัดไป หรือ ใช้ในการ Import Wallet ในเครื่องอื่นๆ



ภาพที่ 18 การรับชุดคำยืนยันบัญชี

ขั้นตอนที่ 6 : คือการยืนยันการจำบันทึกโดยจะต้องคลิกที่คำสั่งตามลำดับชุดคำที่ได้ในขั้นตอนที่ 5 ซึ่งต้องตรงทุกคำจึงจะสำเร็จ



ภาพที่ 19 การยืนยันชุดคำ

### บทที่ 3 การออกแบบ

#### โครงสร้างข้อมูล

##### 1. ผู้ใช้งาน

```

Struct User
- address addressWalletUser;
- uint256 idUser;
- string passwordUser;
- string genderUser;
- string fnameUser;
- string lnameUser;
- string addressUser;
- int dateUser;
- string diseaseUser;
- string medicineUser;
- string phoneUser;
- string idCard;

mapping(address=>User) user;

```

ภาพที่ 20 struct user

ชื่อตัวแปร	ชนิดตัวแปร	เพิ่มเติม
AddressWalletUser	address	เก็บเลข Wallet ของผู้ใช้งาน
idUsser	uint	เลขลำดับที่ของผู้ใช้งาน
passwordUser	string	รหัสผ่านของผู้ใช้งาน
genderUser	string	เพศ
fnameUser	string	ชื่อ
lnameUser	string	นามสกุล
addressUser	string	ที่อยู่ของผู้ใช้งาน

dateUser	int	วันเกิดของผู้ใช้งาน เก็บเป็น timestamp
diseaseUser	string	โรคแทรกซ้อน
medicineUser	string	ยาที่แพ้
phoneUser	string	เบอร์โทรศัพท์
idCard	string	เลขบัตรประชาชน

## 2. ผลการตรวจของผู้ใช้งาน

```

Struct Result
- uint idResult;
- int FPG;
- int HbA1C;
- Pressure pressure;
- Fat fat;
- int BMI;
- int Albumin;
- uint height;
- uint weight;
- string medicine;
- bool keep;

mapping (address => mapping(uint => ResultUser)) resultUser;

```

ภาพที่ 21 struct result

```

Struct Pressure
- int pressureHigh;
- int pressureLow;

```

ภาพที่ 22 struct pressure

```

Struct Fat
- int TG;
- int LDL;
- int HDL;

```

ภาพที่ 23 struct fat



ชื่อตัวแปร	ชนิดตัวแปร	เพิ่มเติม
idResult	uint	เลขที่ของผลตรวจ
FPG	int	ค่า Fasting Blood Sugar
HbA1c	int	ค่า ฮีโมโกลบิน เอ วัน ซี
BMI	int	ค่า BMI
Albumin	int	ค่า albumin
height	uint	ส่วนสูง
weight	uint	น้ำหนัก
medicine	string	ยาที่ได้รับจากการตรวจในครั้งนั้น
keep	bool	ตรวจสอบว่า id ของผลตรวจมีการบันทึกแล้วหรือยัง
pressureHigh	string	ความดันตัวบน
pressureLow	int	ความดันตัวล่าง
TG	int	ค่าไตรกลีเซอไรด์
LDL	int	ค่า LDL
HDL	int	ค่า HDL

### 3. ข้อมูลการจ่ายเงินของผู้ใช้งาน

Struct Pay
- uint idPay; - uint datePay; - uint EXPdate; - bool keep;
mapping(address=> mapping(uint =>Pay)) pay;

ภาพที่ 24 struct pay

ชื่อตัวแปร	ชนิดตัวแปร	เพิ่มเติม
idPay	uint	ครั้งที่จ่าย
datePay	uint	วันที่จ่าย
EXPdate	uint	วันหมดอายุ
keep	bool	ตรวจสอบ id ว่าจ่ายหรือยัง

## ฟังก์ชันหลักในการทำงานกับโครงสร้างข้อมูล

### 1. ข้อมูลผู้ใช้งาน

- addUser() ฟังก์ชันสำหรับเพิ่มข้อมูลของผู้ใช้งาน
- getUser() ฟังก์ชันดึงข้อมูลของผู้ใช้งาน
- checkRegister() ฟังก์ชันสำหรับตรวจสอบว่าเลข wallet ที่ใช้เคยสมัครสมาชิกแล้วหรือยัง
- checkLogin() ฟังก์ชันสำหรับเปรียบเทียบรหัสผ่าน

### 2. ข้อมูลการจ่ายเงิน

- paying() ฟังก์ชันบันทึกข้อมูลการจ่ายเงินในแต่ละครั้ง
- getLastPay() ฟังก์ชันในการดึงข้อมูลการจ่ายเงินล่าสุดของผู้ใช้งาน

### 3. ข้อมูลผลการตรวจ

- addResultUser() ฟังก์ชันในการเพิ่มผลการตรวจของผู้ใช้งานในแต่ละครั้ง
- getResultUserPerId1() ฟังก์ชันในการดึงข้อมูลผลการตรวจแต่ละครั้ง

- showListResult() ฟังก์ชันในการดึงจำนวนผลการตรวจทั้งหมดที่มีของผู้ใช้งาน
- compare<name>() ฟังก์ชันในการเปรียบเทียบเกณฑ์มาตรฐานต่างๆเกี่ยวกับเบาหวาน

## บทที่ 4 ผลการดำเนินการ

การจัดทำโครงการ เรื่อง ระบบสุขภาพส่วนบุคคลที่มีความปลอดภัย โดยระบบถูกพัฒนาขึ้นด้วย Blockchain ตามขั้นตอนข้างต้น และมีผลการดำเนินงานดังนี้

- ระบบการสมัครสมาชิก เมื่อสมัครสมาชิกจะต้องกรอกข้อมูลและจ่ายเงินในตอนสมัคร

ภาพที่ 25 หน้าสมัครสมาชิก

ภาพที่ 26 Login

- การแสดงข้อมูลผู้ใช้

Personal Healthcare ข้อมูลส่วนตัว ผลการตรวจ เพิ่มผลการตรวจ ข้อมูลสุขภาพ คุณคือ ชัยสิทธิ์ [logout](#)

ชัยสิทธิ์ แซ่ส้ม

อายุ	22 ปี
วันเกิด	16 มกราคม พ.ศ. 2541
เพศ	ชาย
เลขบัตรประชาชน	2909801034317
ที่อยู่	452/14
เบอร์โทร	0911676894
โรคประจำตัว	ไม่มี
ประวัติแพ้ยา	ไม่มี
วันหมดอายุสัญญา	27 เมษายน พ.ศ. 2564

ภาพที่ 27 การแสดงข้อมูลผู้ใช้

- การบันทึกข้อมูลผลการตรวจ

Personal Healthcare ข้อมูลส่วนตัว ผลการตรวจ เพิ่มผลการตรวจ ข้อมูลสุขภาพ คุณคือ ชัยสิทธิ์ [logout](#)

เพิ่มข้อมูลผลการตรวจ

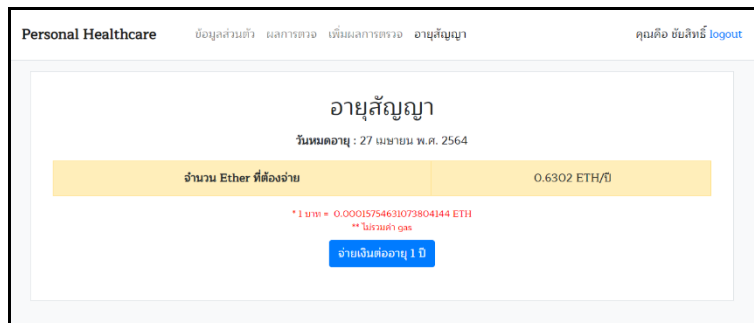
ชัยสิทธิ์ แซ่ส้ม

วันที่ (Date)	<input type="text" value="วว/ดด/ปปปป"/>
ระดับน้ำตาลในเลือด (FPG)	<input type="text" value="00.00"/>
ระดับน้ำตาลเฉลี่ยในเลือด (HBA1C)	<input type="text" value="00.00"/>
ความดัน (Pressure)	<input type="text" value="000"/> / <input type="text" value="00"/>
ไขมันคอเลสเตอรอล (TG)	<input type="text" value="00.00"/>
แอลดีแอล (LDL)	<input type="text" value="00.00"/>
เอชดีแอล (HDL)	<input type="text" value="00.00"/>
สภาวะไขมัน (Albumin)	<input type="text" value="00.00"/>
ส่วนสูง ซม. (Height cm)	<input type="text" value="00.00"/>
น้ำหนัก กก. (Weight kg)	<input type="text" value="00.00"/>
ยาที่ได้รับ (Medicine)	<input type="text" value="Acetaminophen"/>

[บันทึกผล](#)

ภาพที่ 28 การบันทึกข้อมูลผลการตรวจ

- ชำระค่าบริการด้วย Ethereum ชำระเงินครั้งแรกในตอนสมัครสมาชิก และสามารถต่ออายุสัญญาเพิ่มได้ครั้งละ 1 ปี



ภาพที่ 29 ชำระค่าบริการด้วย Ethereum

- แสดงข้อมูลการตรวจและสถานะของโรค มีการเปรียบเทียบค่าในแต่ละค่า แล้วแสดงผล

<div> Personal Healthcare ข้อมูลส่วนตัว ผลการตรวจ เก็บผลการตรวจ อายุสัญญา <div>คุณคือ ชัยสิทธิ์ <a href="#">logout</a></div> </div>		
<div> <div>วันที่ 09 เมษายน พ.ศ. 2563</div> <div>ชัยสิทธิ์ แซ่ลิ้ม</div> </div>		
วันที่ (Date)	09 เมษายน พ.ศ. 2563	สถานะ
ระดับน้ำตาลในเลือด (FPG)	20.25 มก./ดล.	ต่ำกว่ามาตรฐาน
ระดับน้ำตาลเฉลี่ยในเลือด (HbA1C)	10.3 %	สูงกว่ามาตรฐาน
ความดัน (Pressure)	185/78 มม./ปรอท	สูงกว่ามาตรฐาน
ไตรกลีเซอไรด์ (TG)	10 มก./ดล.	สูงกว่ามาตรฐาน
แอลดีแอล (LDL)	15 มก./ดล.	ปกติ
เอชดีแอล (HDL)	5 มก./ดล.	ต่ำกว่ามาตรฐาน
สารโปรตีน (Albumin)	3.33 มก./ลิตร.	ปกติ
BMI	17.96	ต่ำกว่ามาตรฐาน
ส่วนสูง ซม. (Height cm.)	175 ซม.	
น้ำหนัก กก. (Weight kg.)	55 กก.	
ยาที่ได้รับ (Medicine)		

ภาพที่ 30 แสดงข้อมูลการตรวจและสถานะของโรค

## บทที่ 5 สรุปผลการดำเนินงาน และข้อเสนอแนะ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาเทคโนโลยี blockchain และนำมาพัฒนาระบบสุขภาพส่วนบุคคลที่มีความปลอดภัย มีผลการศึกษาดังนี้

Blockchain เป็น open source ที่เปิดให้นักพัฒนาสามารถนำไปพัฒนาได้ฟรีไม่มีค่าใช้จ่ายในการพัฒนา แต่มีค่าใช้จ่ายในการใช้งานจริงและรูปแบบของภาษามีความคล้ายคลึงกับ java script และการนำไปใช้บน web application โดยใช้ api ของ Ethereum เป็นตัวกลางในการเชื่อมต่อระหว่าง หน้า web site กับ blockchain เพื่อบันทึก หรือ แสดงผลตามที่ได้เขียนไว้

พัฒนาระบบสุขภาพส่วนบุคคลที่มีความปลอดภัย ที่มาพร้อมกันประกันสุขภาพ โดยผู้ใช้งานสามารถซื้อ และได้รับการคุ้มครองทันทีที่ชำระเงิน โดยไม่ต้องผ่านคนกลางนายหน้า หรือ รออนุมัติให้เสียเวลา เพราะเราใช้ Smart contract ซึ่งเป็นหนึ่งในคุณสมบัติของ Blockchain ที่จะทำงานโดยอัตโนมัติภายใต้เงื่อนไขที่กำหนดไว้ และผู้ใช้งานสามารถเข้าถึงระบบได้ทุกที่ผ่าน web browser เพื่อบันทึก หรือ ดูผลการรักษาที่ผ่านมา หรือเอาไปยื่นให้กับแพทย์ที่กำลังจะรักษาเพื่อความรวดเร็วในการรักษา ลดขั้นตอนการทำงานของแพทย์ พยาบาล อีกทั้งระบบยังแสดงถึงสถานะของโรคที่กำลังเป็นอยู่ว่าอยู่ในระดับไหน มีความเสี่ยงในจุดใดเพื่อให้ผู้ใช้ได้ตระหนักถึงสุขภาพปัจจุบันที่กำลังเป็นอยู่และดูแลสุขภาพตนเองได้มากขึ้น

### ข้อเสนอแนะ

จากการศึกษาพัฒนา Blockchain Ethereum ทำให้ทราบว่าพัฒนานา blockchain นั้นต้องมีความรู้ด้าน java scripts และ solidity ในระดับหนึ่งและการใช้งานมีข้อจำกัดในเรื่องค่าใช้จ่ายในการใช้งานจริงจึงเหมาะที่จะใช้กับ Project ที่ต้องการความสำคัญทางด้านการเก็บข้อมูลเช่น การเงินธนาคาร ประวัติการรักษาโรงพยาบาล ทะเบียนราษฎร์ เป็นต้น

## บรรณานุกรม

- พ.อ.ดร.เศรษฐพงศ์ มะลิสุวรรณ 4 เมษายน 2017 วิวัฒนาการของ Blockchain สืบค้นเมื่อ 2 พ.ย. 2562 จาก <https://www.it24hrs.com/2017/blockchain-evolution/?fbclid=IwAR2HomegFhmaXccKULLy2glj-B1NXObSUGqW-griA10mHiLpvV5fRUGCweI>
- Worannittawan 2019 Ethereum คืออะไร และมีความสำคัญในโลก Blockchain อย่างไร สืบค้นเมื่อ 2 พ.ย. 2562 จาก <https://bit.ly/350ySqK>
- บทความจากนิตยสาร Eleader ฉบับเดือน พฤษภาคม 2559. จาก <https://www.uih.co.th/th/knowledge/blockchain-is?fbclid=IwAR3GU42LHe4AYD1DXbYRDVbtAsEiqxhsjbqRoeyLydCiyFs-ZEEg7pi2X0>
- เขียนโดย Alyssa Hertig , รูปภาพโดย Maria Kuznetsov. (2019) Ethereum คืออะไร. สืบค้นเมื่อ 4 พ.ย. 2562. จาก <https://www.coindesk.com/information/what-is-ethereum>
- Jedsada Tiwongvorakul. (2018) มารู้จักกับ Solidity ขั้นพื้นฐานร่วมกัน. สืบค้นเมื่อ 4 พ.ย. 2562. จาก <https://bit.ly/2XbC67Z>
- Gary. (2018). Developing Ethereum Smart Contracts for Beginners. สืบค้นเมื่อ 6 พ.ย. 2562. จาก <https://bit.ly/2CH20a5>
- Pongsatorn Tonglairoom. (2018). สร้าง Smart Contract อย่างง่าย. สืบค้นเมื่อ 10 พ.ย. 2019. จาก <https://bit.ly/350yYyC>
- Thansettakij (2019) ความเป็นส่วนตัว (Privacy) บนเทคโนโลยีบล็อกเชน (Blockchain) สืบค้นเมื่อวันที่ 13 ธ.ค. 2019 จาก <https://www.thansettakij.com/content/416232>
- กองโรคไม่ติดต่อ (2019) จำนวนและอัตราการตายโรคไม่ติดต่อ ปี 2559-2561 สืบค้นเมื่อ 2 ก.พ. 2020 <http://www.thaincd.com/2016/mission/documents-detail.php?id=13653&tid=32&gid=1-020>

Pobpad (2017)โรคเบาหวาน สืบค้นเมื่อ 5 ก.พ.2020

<https://www.pobpad.com/%E0%B9%82%E0%B8%A3%E0%B8%84%E0%B9%80%E0%B8%9A%E0%B8%B2%E0%B8%AB%E0%B8%A7%E0%B8%B2%E0%B8%99>

สมัชชาสุขภาพแห่งชาติ(2018)การพัฒนาระบบบริการสุขภาพอย่างมีส่วนร่วม สืบค้นเมื่อ 3 มี.ค.2020

<https://kbphpp.nationalhealth.or.th/bitstream/handle/123456789/3260/%E0%B8%AB%E0%B8%A5%E0%B8%B1%E0%B8%81%208.3.pdf?sequence=3&isAllowed=y&fbclid=IwAR00Jev7EYT9wjhkJQb01Semi40Az8LhjPPdoas7y0KMpqTTUym2z3Fw73c>