

หลักสูตรที่ 5

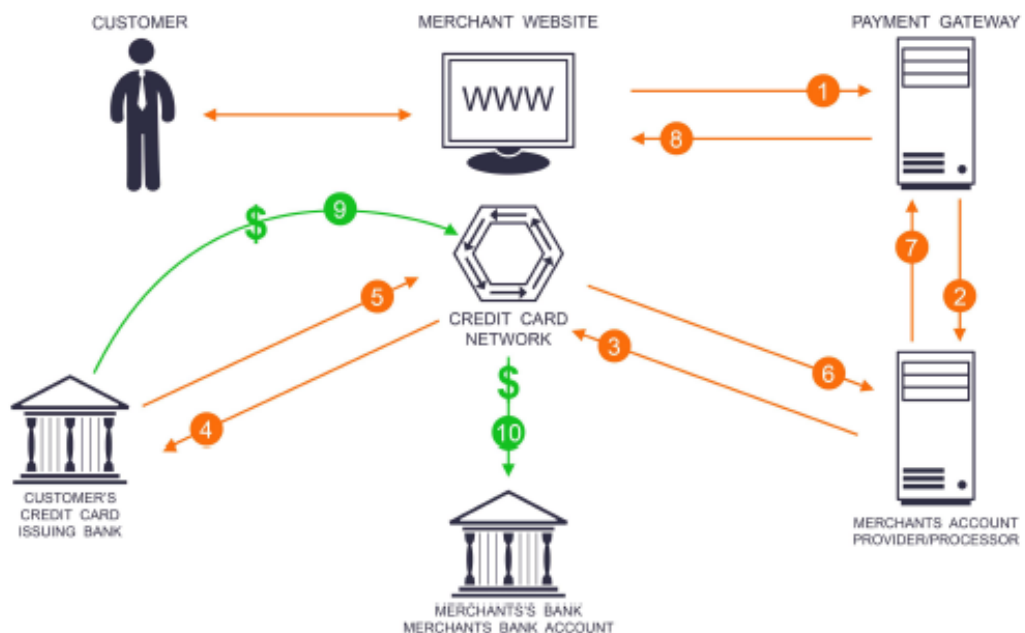
Blockchain Technology for Developers

จัดโดย บริษัท ไอเอ็มซี เอ้าท์ซอร์ซซิง (ประเทศไทย) จำกัด

ระหว่างวันที่ 30 – 31 สิงหาคม 2560

วิทยากร : อาจารย์ธีรชัย เหลาทอง

ในการทำธุรกรรมออนไลน์โดยทั่วไป ที่ต้องมีการจ่ายชำระเงินด้วยบัตรเครดิต มีขั้นตอนมากมายและต้องการความมั่นคงปลอดภัยสูง ต้องมีระบบศูนย์กลาง (centralized system) ซึ่งเปรียบเสมือนเป็นคนกลางทำหน้าที่ควบคุมดูแลการกระทำที่เกิดขึ้นทั้งหมด ดังนี้



บล็อกเชน (Blockchain) คือ ระบบโครงข่ายในการเก็บบัญชีธุรกรรมออนไลน์ ซึ่งมีลักษณะเป็นเครือข่ายแบบกระจายศูนย์ ที่เก็บสถิติการทำธุรกรรมทางการเงิน และสินทรัพย์ชนิดอื่น ๆ อีกในอนาคต **โดยไม่มีตัวกลางคือสถาบันการเงินหรือสำนักชำระบัญชี** ระบบ Blockchain จะไม่มีตัวกลางอย่างที่เคยเป็นมา ยกตัวอย่างการทำธุรกรรมด้วย Bitcoin จะมีรหัส Token สร้างขึ้นมาเพื่อสื่อสารกับ Blockchain และทำการตรวจสอบว่า Bitcoin นั้น ๆ มีความน่าเชื่อถือหรือไม่ก่อนที่จะทำธุรกรรมให้สำเร็จต่อไป

Blockchain จึงเป็นระบบโครงข่ายในการทำธุรกรรมต่าง ๆ ซึ่งตัดตัวกลางอย่างสถาบันการเงินที่มีอยู่ในโลกปัจจุบันออกไป ทำให้ต้นทุนการทำธุรกรรมถูกลง และอาจส่งผลให้สถาบันการเงินที่เป็นตัวกลาง รวมไปถึงสำนักชำระบัญชีต่าง ๆ ไม่จำเป็นต้องมีอีกในอนาคต หากเทคโนโลยีนี้เข้ามาแทนที่ได้อย่างสมบูรณ์

Blockchain ไม่เพียงมีบทบาทอยู่แค่การทำธุรกรรมทางการเงินเท่านั้น แต่ยังนำไปใช้ในงานอื่น ๆ เช่น การเก็บสถิติการเลือกตั้งให้มีความโปร่งใสมากขึ้น การให้ยืม Cloud Storage ระหว่างกัน ระบบ Peer to Peer Lending และอื่น ๆ อีกมากมาย ซึ่งแม้แต่เหล่าธนาคารเองก็ตัดสินใจเข้าลงทุนในการทำ Blockchain มากขึ้น โดยล่าสุด สถาบันการเงินอย่างธนาคาร Citibank ตลาดหลักทรัพย์ NASDAQ รวมไปถึงบริษัท VISA ได้เข้าลงทุนในบริษัทบล็อกเชนชั้นนำอย่าง Chain.com เพื่อเข้าสู่แนวทางรักษาดตลาดเทคโนโลยีนี้เช่นกัน

Blockchain มีการพัฒนาใหม่ ๆ ไปสู่การใช้งานที่มากกว่าการทำธุรกรรม Bitcoin (สกุลเงินดิจิทัล ที่สร้างขึ้นโดย Satoshi Nakamoto ซึ่งเป็นชื่อสมมติของบุคคลที่ยังไม่มีใครทราบตัวตนที่แท้จริง) ในอดีตที่ไม่ได้รับการยอมรับ ผ่นวกรวมกับกระแสการเพิ่มขึ้นของอุปกรณ์ที่ใช้แนวคิด อินเทอร์เน็ต ออฟ ธิงส์ (Internet of Things) จำเป็นต้องมีการจัดการและดูแลรักษาความมั่นคงปลอดภัยระหว่างอุปกรณ์ต่าง ๆ และความจำเป็นที่จะต้องบันทึกฐานข้อมูลของการติดต่อต่าง ๆ เหล่านั้น ทำให้เทคโนโลยี Blockchain ที่ให้ความสำคัญกับความเป็นส่วนตัว จะกลายเป็นตัวช่วยสำคัญของการใช้งานดังกล่าว โดยลดขั้นตอนในระบบการทำงานให้เรียบง่ายขึ้น มีความยืดหยุ่นสูงขึ้น รวมทั้งการตอบสนองความต้องการของลูกค้าได้อย่างรวดเร็ว

Bitcoin ได้สร้างแนวคิดที่ว่า ไม่ต้องมีคนกลางทำหน้าที่ควบคุมดูแล แต่ใช้ Blockchain แทนข้อมูลใด ๆ ก็ตาม เมื่อนำเข้ากระบวนการนี้ สามารถพิสูจน์/บอกได้ว่า นำเข้าโดยใคร (Digital Fingerprint) ซึ่งไม่สามารถเปลี่ยนแปลงแก้ไขได้และไม่สามารถปฏิเสธการกระทำ



Source:
<https://en.wikipedia.org/wiki/Bitcoin>

Digital Signature มีคุณสมบัติเหมือนลายเซ็นในโลกแห่งความจริง ซึ่งมีเพียงเจ้าของลายเซ็นเท่านั้นที่เซ็นได้ และเมื่อเซ็นแล้วจะมีผลผูกพันกับเอกสารที่ถูกลงนามนั้นเท่านั้น

การทำงานของ Digital Signature มีขั้นตอนการทำงานดังนี้

1. เจ้าของลายเซ็นสร้าง secret key และ public key ของตนเองขึ้น
2. เจ้าของลายเซ็นนำ secret key มาเซ็นลงในเอกสาร message ได้เป็นเอกสารใหม่ชื่อ sig
3. นำเอกสาร sig ส่งให้ฝ่ายอื่นๆ ที่เกี่ยวข้อง
4. ฝ่ายที่เกี่ยวข้องนำ public key ของเจ้าของลายเซ็นพร้อมกับ message และเอกสาร sig มาพิสูจน์

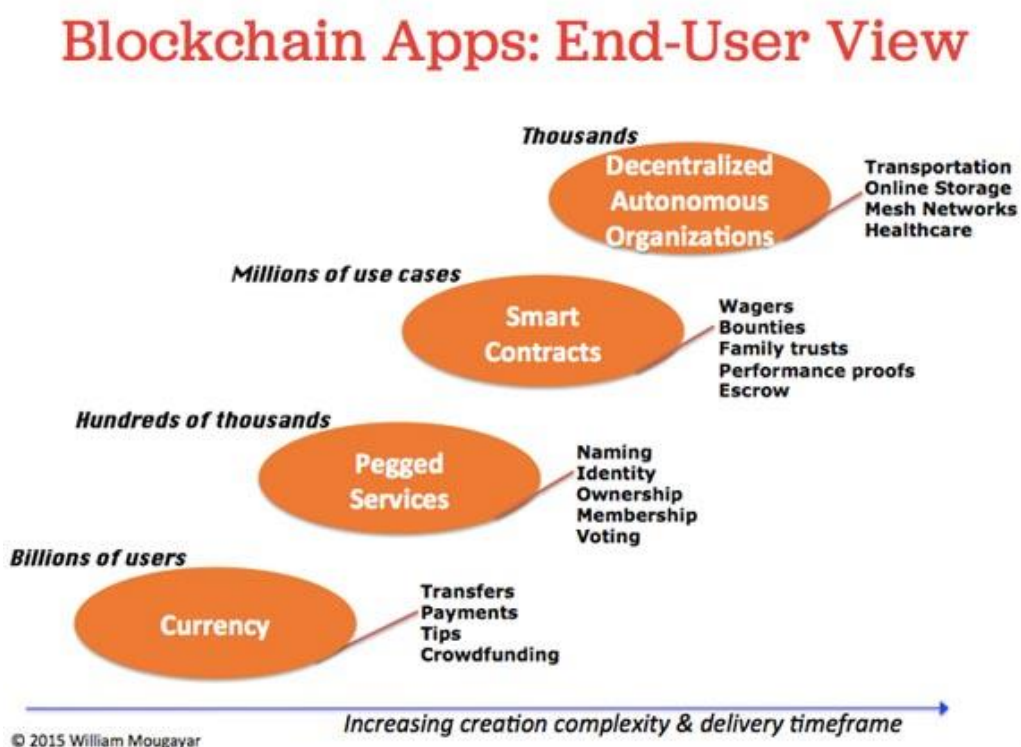
หากเอกสาร sig มาจากลายเซ็นที่ถูกต้อง ก็จะยอมรับเอกสาร sig นั้นว่าได้ผ่านการลงนามที่ถูกต้อง

ซึ่งหากเอกสาร message คือ Hash Pointer ของ Blockchain ใดๆ หมายความว่า เจ้าของลายเซ็นสามารถเซ็นกำกับข้อมูลใน Blockchain และเป็นการพิสูจน์ว่า Blockchain ก่อนหน้าเป็นข้อมูลที่ต้องการและสามารถพิสูจน์ได้ว่ามีใครแก้ไขข้อมูลในภายหลังหรือไม่

นอกจากนี้ public key ยังถูกใช้เป็น identity เพื่อระบุตัวตนของผู้ใช้ Blockchain ดังนั้น การใช้ secret key เซ็น message ใดๆ จะเป็นการระบุว่าผู้นั้นได้ยอมรับ message นั้นว่าเป็นความจริงอีกด้วย

ความสำเร็จของ Blockchain จะสามารถพลิกสถานะการให้บริการด้านการเงินในโลกดิจิทัลได้หรือไม่ การหาพาร์ทเนอร์ที่มีประสบการณ์ในการทำงานกับระบบความซับซ้อนและความหลากหลาย ในทุกระดับการใช้ งานไม่ว่าเล็กหรือใหญ่ เป็นหัวใจสำคัญของการจัดการกับปัญหานี้ได้อย่างดีที่สุด ซึ่งถ้าย้อนกลับไปเมื่อ 5 ปีที่ผ่านมา แนวคิดทางธุรกิจเหล่านี้ต่างเคยถูกมองว่าเป็นเรื่องที่ไม่น่าจะเกิดขึ้นได้จริง หากแต่ปัจจุบันเรื่องเหล่านี้ได้กลายเป็นตัวกำหนดผู้ชนะในอนาคต ซึ่งทั้งหมดนี้สามารถเกิดขึ้นได้ด้วยการมองว่าซอฟต์แวร์คือตัวแปรสำคัญของการเปลี่ยนแปลงของโลกยุคใหม่นั้นเอง

มีการนำ Blockchain ไปใช้งานเพิ่มขึ้นตามลำดับ ดังนี้



ตัวอย่างการประยุกต์ Blockchain ในองค์กรต่าง ๆ ดังนี้

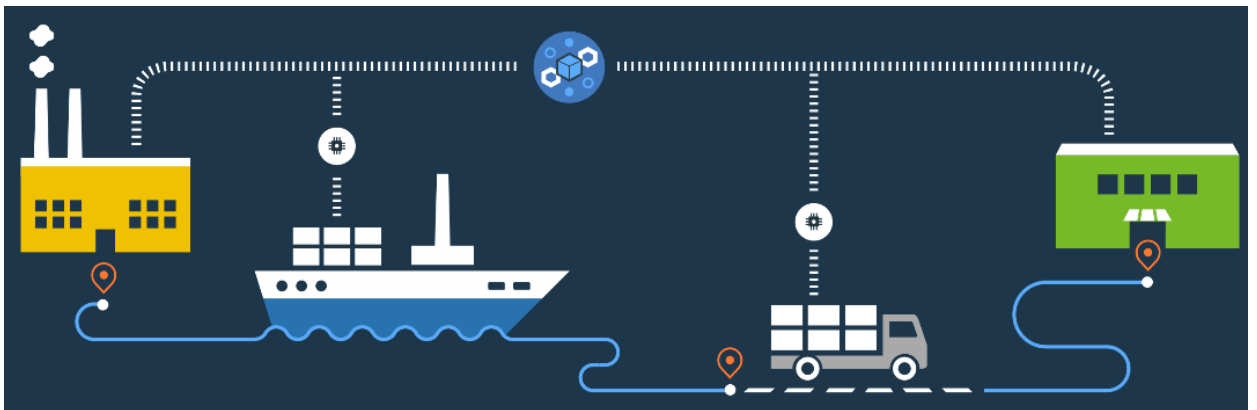


ตัวอย่าง

Blockchain สาธารณะ

Blockchain ขององค์กรธุรกิจ

ตัวอย่าง การประยุกต์ Blockchain ในกระบวนการส่งเซอรี



กระบวนการส่งเซอรี ผ่านขั้นตอนการขนส่ง โดยควบคุมอุณหภูมิไม่ให้เกิน 0 องศา เมื่อมีการเปลี่ยนมือระหว่างผู้ขนส่ง จะมีการส่งข้อมูลอุณหภูมิ (log) ดังนั้น ความรับผิดชอบของผู้ขนส่งจะถูกโอนถ่ายไปเป็นทอดๆ เช่น เมื่อพบว่าอุณหภูมิเกิน 0 องศา ในระหว่างการขนส่งด้วยรถบรรทุก ข้อมูลจะถูกส่งไปยัง Blockchain