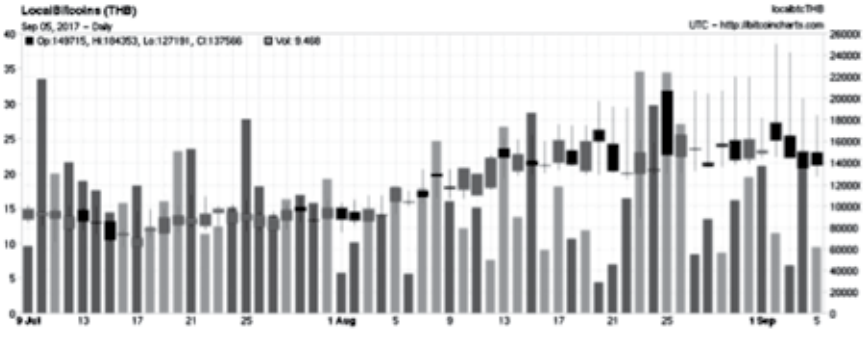
ทำความรู้จักกับ Blockchain และเตรียมรับมือ FINTECH

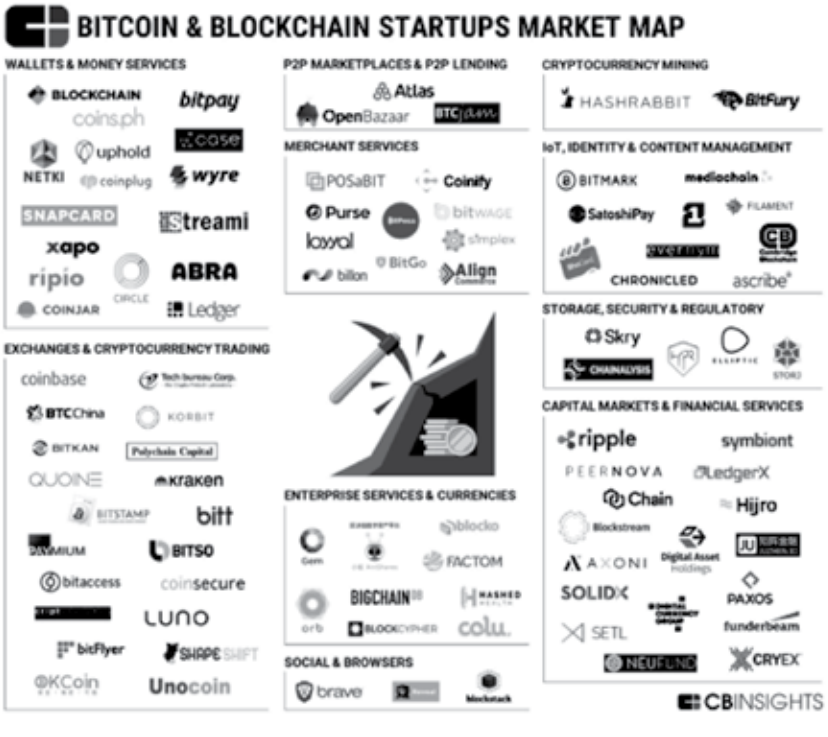
วิชย์ศุทธ์ เมาะพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

ด้วยอัตราการเติบโต และความนิยมของ Bitcoin จึงเกิดตลาดแลกเปลี่ยน Bitcoin ซึ่งมูลค่าขึ้นอยู่กับความต้องการใช้งาน Bitcoin ในการแลกเปลี่ยนซื้อ-ขาย คล้ายๆ กับตลาดทุนที่เราคุ้นเคย ถ้ามีคนต้องการขายมากกว่าซื้อมูลค่าจะลดลง กลับกันถ้ามีปริมาณการซื้อมากกว่าขายมูลค่าก็จะเพิ่มขึ้น แต่จะมีการกำหนดเพดานจำนวน Bitcoin ไว้ว่าถ้าถึง 21 ล้าน Bitcoin จะไม่สามารถเพิ่มได้อีก เพื่อป้องกันปัญหาการเฟ้อของ Bitcoin ปัจจุบันมีองค์การภาคเอกชนเข้ามาดำเนินงานเกี่ยวข้องกับการจัดการแลกเปลี่ยน Bitcoin และแลกเปลี่ยน Bitcoin เป็นเงินตราสกุลต่างๆ อยู่ทั่วโลก รวมถึงการทำหน้าที่เป็นตัวแทนเพื่อจัดการเรื่องประเป๋าเงินหรือ Bitcoin wallet

คราวนี้ เราจะมากล่าวถึงเทคโนโลยีที่อยู่เบื้องหลัง Bitcoin นั่นคือ Blockchain กัน กลไกการทำงานของ Blockchain นั้นอย่างที่กล่าวไว้ว่าเป็นระบบแบบกระจายโดยมีการประกาศการทำธุรกรรมไปยัง Node ต่างๆ ในเครือข่ายแบบสาธารณะแทนการนำมาจัดเก็บไว้ที่ส่วนกลาง โดยแต่ละ Node หรือแต่ละคนจะถือสมุดบัญชีของตัวเองไว้ เมื่อถึงตรงนี้ก็เกิดคำถามว่าแล้วจะเกิดความไว้วางใจกันได้อย่างไร เพราะปกติแล้ว





ในสมุดบัญชีจะมียอดเงินปรากฏอยู่แล้วยิ่งต่างคนต่างถือก็กลายเป็นว่าถ้ามีใครแก้ตัวเลขยอดเงินในสมุดบัญชีของตัวเองล่ะ สำหรับกลไกของ Blockchain ตัวอย่างการทำงานร่วมกับ Bitcoin ก็คือในสมุดบัญชีจะไม่ปรากฏยอดเงินจะมีแต่เลขที่บัญชี (Address) ลายเซ็นต์อิเล็กทรอนิกส์ (Digital Signature) ของเจ้าของบัญชี และรายการธุรกรรม (Transaction) ที่เกิดขึ้น โดยจัดเก็บในสมุดบัญชีสาธารณะ (Public ledger) ที่รวมรายการธุรกรรมที่เกิดขึ้นทั้งหมดในระบบ Blockchain ซึ่งแต่ละคนก็จะถือไว้เช่นกัน โดยเลขที่บัญชีของแต่ละคนหรือแต่ละ Node จะไม่ซ้ำกัน เพราะจะถูกสร้างขึ้นมาจากการนำเอาลายเซ็นต์อิเล็กทรอนิกส์มาเข้ากระบวนการคำนวณทางคณิตศาสตร์ ออกมาเป็นเลขบัญชี ซึ่งไม่สามารถนำเอาเลขบัญชีมาย้อนกระบวนการเพื่อกลับไปเป็นลายเซ็นต์อิเล็กทรอนิกส์ได้ ทำให้มีความปลอดภัยค่อนข้างสูง เนื่องจากการทำธุรกรรมอย่างที่ทราบต้องใช้ลายเซ็นต์ของผู้ทำธุรกรรมเป็นเครื่องยืนยันการทำธุรกรรมนั้นๆ ในทางอิเล็กทรอนิกส์ก็เช่นเดียวกัน แต่เปลี่ยนมาใช้เป็นลายเซ็นต์อิเล็กทรอนิกส์แทน

กระบวนการต่อมาเมื่อมีการทำธุรกรรมเกิดขึ้น เนื่องจากไม่มีกลไกของคนกลางคือธนาคาร หรือสถาบันการเงินเข้ามาช่วยจัดการทำให้นอกเหนือจากคู่ของ node หรือคนที่มีการทำธุรกรรมระหว่างกันจะมี node อื่นๆ เข้ามามีส่วนร่วมในการยืนยันว่าการทำธุรกรรมนั้นๆ เกิดขึ้นจริง และเกิดขึ้นอย่างถูกต้องโดยการตรวจสอบย้อนกลับไปยัง node ที่จัดเก็บข้อมูลการทำธุรกรรมก่อนหน้าที่จะเกิดธุรกรรมในปัจจุบันของคู่ที่ทำธุรกรรมทั้ง 2 ฝ่าย ตัวอย่างเช่น นาย A จะโอนเงินให้ นาย B จำนวน 50 Bitcoin โดยมีนาย C และ D เป็นผู้ตรวจสอบข้อมูลเพื่อยืนยันการทำธุรกรรมดังกล่าว โดยเมื่อทำการตรวจสอบแล้วพบว่าก่อนหน้านี้นาย A เคยทำธุรกรรมกับนาย K โดยนาย K โอนเงินให้ จำนวน 30 Bitcoin เป็นค่าจ้างออกแบบ website และนาย A ก็ได้ทำธุรกรรมกับนางสาว L โดยนางสาว L ได้โอนเงินให้นาย A 25 Bitcoin เป็นค่าเช่าห้องพัก ทำให้นาย A มียอดเงินเพียงพอที่จะโอนให้นาย B ในธุรกรรมปัจจุบันที่กำลังเกิดขึ้น (ประวัติการทำธุรกรรมที่เกิดขึ้นแต่ละครั้งจะเสมือนการเขียนเช็ค คือ เมื่อต้องการโอนเงินจะเป็นการเขียนเช็คสั่งจ่ายให้กับคู่ธุรกรรมหากมียอดเงินคงเหลือระบบจะสั่งเขียนเช็คของยอดเงินคงเหลือสั่งจ่ายตัวผู้ทำธุรกรรมเอง จึงเป็นลักษณะที่ว่าเราได้รับเช็คมาแล้วจะนำยอดเงินที่ได้รับไปใช้ต่อจะต้องเขียนเช็คขึ้นมาอย่างน้อย 2 ฉบับ นั่นคือเช็คที่สั่งจ่ายกับเช็คที่เป็นเงินทอนกลับเข้าบัญชีของตัวเองเพื่อกระทบยอด)

คำถามต่อมาคือนาย C และ D เป็นใครมาจากไหน

นาย C และ D เป็นผู้ใช้งาน Bitcoin เหมือนนาย A กับนาย B เข้าร่วมเชื่อมต่อเครือข่าย Bitcoin Blockchain แต่คราวนี้ไม่ได้มีบทบาทเป็นผู้ทำธุรกรรมแต่เป็นผู้ตรวจสอบ และยืนยันการทำธุรกรรมในภาษาของ Blockchain จะเรียกว่า Miner (นักขุดเหมือง) ที่เราจะเคยได้ยินบ่อยๆ ว่านักขุด Bitcoin โดย Miner จะได้ค่าตอบแทนเป็น Bitcoin ภายหลังจากได้ทำการยืนยันธุรกรรมที่เกิดขึ้นเสร็จสมบูรณ์และน่าเชื่อถือ ซึ่งก็มาจากค่าธรรมเนียมในการทำธุรกรรมที่นาย A จ่ายนั่นเอง ด้วยค่าตอบแทนที่เป็น Bitcoin ซึ่งมีมูลค่าค่อนข้างสูงและไม่ค่อยผันผวนเมื่อแลกเป็นเงินสกุลต่างๆ จึงเป็นแรงจูงใจให้เกิด Miner จำนวนมาก แล้ว Miner ต้องใช้ทรัพยากรอะไรในการขุดบ้าง

อ่านต่อฉบับหน้า