

ทำความเข้าใจกับ

Blockchain และเตรียมรับมือ FINTECH



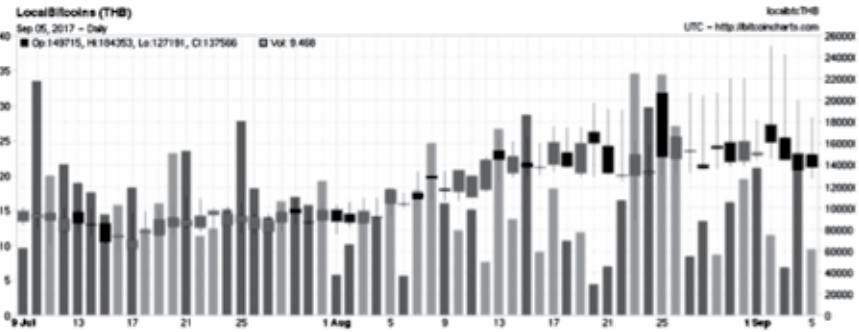
วิษณุคุณท์ เฌงระเพณีย์

ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยเทคโนโลยีกับธุรกิจ
แห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

ด้วย อัตราการเติบโต และความนิยมของ Bitcoin จึงเกิดตลาดแลกเปลี่ยน Bitcoin ซึ่งมูลค่าขึ้นอยู่กับความต้องการใช้งาน Bitcoin ในการแลกเปลี่ยนซื้อ-ขาย คล้ายๆ กับตลาดหุ้นที่เราคุ้นเคย ถ้ามีคนต้องการขายมากกว่าซื้อมูลค่าจะลดลง กลับกันถ้ามีปริมาณการซื้อมากกว่าขายมูลค่าก็จะเพิ่มขึ้น แต่จะมีการกำหนดเพดานจำนวน Bitcoin ไว้ว่า ถ้าถึง 21 ล้าน Bitcoin จะไม่สามารถเพิ่มได้อีก เพื่อป้องกันปัญหาการฟลอปของ Bitcoin ปัจจุบันมีองค์กรภาคเอกชนเข้ามาดำเนินงานเกี่ยวข้องกับการจัดการแลกเปลี่ยน Bitcoin และแลกเปลี่ยน Bitcoin เป็นเงินตราสกุลต่างๆ อยู่ทั่วโลก รวมถึงการทำหน้าที่เป็นตัวแทนเพื่อจัดการเรื่องกระเป๋าเงินหรือ Bitcoin wallet

คราวนี้เราจะมากล่าวถึงเทคโนโลยีที่อยู่เบื้องหลัง Bitcoin นั่นคือ Blockchain กัน กลไกการทำงานของ Blockchain นั้นอย่างที่กล่าวไว้ว่าเป็นระบบแบบกระจายโดยมีการประกาศการทำธุรกรรมไปยัง Node ต่างๆ ในเครือข่ายแบบสาธารณะแทนการนำมาจัดเก็บไว้ที่ส่วนกลางโดยแต่ละ Node หรือแต่ละคนจะถือสมุดบัญชีของตัวเองไว้ เมื่อถึงตรงนี้ก็เกิดคำถามว่าแล้วจะเกิดความไว้วางใจกันได้อย่างไร เพราะปกติแล้ว



BITCOIN & BLOCKCHAIN STARTUPS MARKET MAP

WALLETS & MONEY SERVICES BLOCKCHAIN, bitpay, coins.ph, uhold, NETKI, coinplug, SNAPCARD, Streami, xapo, ripio, COINJAR, Ledger	P2P MARKETPLACES & P2P LENDING Atlas, OpenBazaar, BTCJAFFY	CRYPTOCURRENCY MINING HASHRABBIT, BitFury
EXCHANGES & CRYPTOCURRENCY TRADING coinbase, Tech Bureau Corp., BTCChina, KOBBIT, BITKAN, Polyrails Capital, QUONE, KRAKEN, BITSTAMP, bitt, DYNAMIUM, BITSO, bitaccess, coinsecure, bitfyer, bitFlyer, UNOCOIN, OKCoin	MERCHANT SERVICES POSaBIT, Coinify, Purse, loyal, BitGo, Align Commerce	IoT, IDENTITY & CONTENT MANAGEMENT BITMARK, mediachain, SatoshiPay, FILAMENT, CHRONICLED, ascribe
ENTERPRISE SERVICES & CURRENCIES blocko, FACTOM, BIGCHAIN, BLOCCYPER, colu	STORAGE, SECURITY & REGULATORY Skry, CHANALYSIS, ELASTIC, STORJ	CAPITAL MARKETS & FINANCIAL SERVICES ripple, symbiont, PEERNOVA, LedgerX, Chain, Hijro, Blockstream, Digital Asset Holdings, AXONI, SOLIDIX, SETL, NEUFUND, CRYEX, funderbeam
SOCIAL & BROWSERS brave, Market		CBINSIGHTS

ในสมุดบัญชีจะมียอดเงินปรากฏอยู่แล้วยิ่งต่างคนต่างถือก็กลายเป็นว่าถ้ามีใครแก้ตัวเลขยอดเงินในสมุดบัญชีของตัวเองล่ะ สำหรับกลไกของ Blockchain ตัวอย่างการทำงานร่วมกับ Bitcoin ก็คือในสมุดบัญชีจะไม่ปรากฏยอดเงินจะมีแต่เลขที่บัญชี (Address) ลายเซ็นดิจิทัลอิเล็กทรอนิกส์ (Digital Signature) ของเจ้าของบัญชี และรายการธุรกรรม (Transaction) ที่เกิดขึ้น โดยจัดเก็บในสมุดบัญชีสาธารณะ (Public ledger) ที่รวมรายการธุรกรรมที่เกิดขึ้นทั้งหมดในระบบ Blockchain ซึ่งแต่ละคนก็จะถือไว้เช่นกัน โดยเลขที่บัญชีของแต่ละคนหรือแต่ละ Node จะไม่ซ้ำกัน เพราะจะถูกสร้างขึ้นมาจากการนำเอาลายเซ็นดิจิทัลอิเล็กทรอนิกส์มาเข้ากระบวนการคำนวณทางคณิตศาสตร์ ออกมาเป็นเลขบัญชี ซึ่งไม่สามารถนำเอาเลขบัญชีมาย้อนกระบวนการเพื่อกลับไปเป็นลายเซ็นดิจิทัลอิเล็กทรอนิกส์ได้ ทำให้มีความปลอดภัยค่อนข้างสูง เนื่องจากการทำธุรกรรมอย่างที่ทราบต้องใช้ลายเซ็นของผู้ทำธุรกรรมเป็นเครื่องยืนยันการทำธุรกรรมนั้นๆ ในทางอิเล็กทรอนิกส์ก็เช่นเดียวกัน แต่เปลี่ยนมาใช้เป็นลายเซ็นดิจิทัลอิเล็กทรอนิกส์แทน

กระบวนการต่อมาเมื่อมีการทำธุรกรรมเกิดขึ้น เนื่องจากไม่มีกลไกของคนกลางคือธนาคาร หรือสถาบันการเงินเข้ามาช่วยจัดการทำให้ออกเหนือจากคู่ของ node หรือคนที่มีการทำธุรกรรมระหว่างกัน จะมี node อื่นๆ เข้ามามีส่วนร่วมในการยืนยันว่าการทำธุรกรรมนั้นๆ เกิดขึ้นจริง และเกิดขึ้นอย่างถูกต้องโดยการตรวจสอบย้อนกลับไปยัง node ที่จัดเก็บข้อมูลการทำธุรกรรมก่อนหน้าที่จะเกิดธุรกรรมในปัจจุบันของคู่ที่ทำธุรกรรมทั้ง 2 ฝ่าย ตัวอย่างเช่น นาย A จะโอนเงินให้ นาย B จำนวน 50 Bitcoin โดยมีนาย C และ D เป็นผู้ตรวจสอบข้อมูลเพื่อยืนยันการทำธุรกรรมดังกล่าว โดยเมื่อทำการตรวจสอบแล้วพบว่าก่อนหน้านี้ นาย A เคยทำธุรกรรมกับนาย K โดยนาย K โอนเงินให้จำนวน 30 Bitcoin เป็นค่าจ้างออกแบบ website และนาย A ก็ได้ทำธุรกรรมกับนางสาว L โดยนางสาว L ได้โอนเงินให้นาย A 25 Bitcoin เป็นค่าเช่าห้องพัก ทำให้นาย A มียอดเงินเพียงพอที่จะโอนให้นาย B ในธุรกรรมปัจจุบันที่กำลังเกิดขึ้น (ประวัติการทำธุรกรรมที่เกิดขึ้นแต่ละครั้งจะเสมือนการเขียนเช็ค คือ เมื่อต้องการโอนเงินจะเป็นการเขียนเช็คส่งจ่ายให้กับคู่ธุรกรรมหากมียอดเงินคง

เหลือระบบจะสั่งเขียนเช็คของยอดเงินคงเหลือส่งจ่ายตัวผู้ทำธุรกรรมเอง จึงเป็นลักษณะที่ว่าเราได้รับเช็คมาแล้วจะนำยอดเงินที่ได้รับไปใช้ต่อจะต้องเขียนเช็คขึ้นมาอย่างน้อย 2 ฉบับ นั่นคือเช็คที่ส่งจ่ายกับเช็คที่เป็นเงินทอนกลับเข้าบัญชีของตัวเองเพื่อกระทบยอด)

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 ภายหลังจากได้ทำการยืนยันธุรกรรมที่เกิดขึ้นเสร็จสมบูรณ์และนำเช็ถือือ ซึ่งก็มาจากค่าธรรมเนียมในการทำธุรกรรมที่นาย A จ่ายนั่นเอง ด้วยค่าตอบแทนที่เป็น Bitcoin ซึ่งมีมูลค่าค่อนข้างสูงและไม่ค่อยผันผวนเมื่อแลกเป็นเงินสดหลายๆ จึงเป็นแรงจูงใจให้เกิด Miner จำนวนมาก แล้ว Miner ต้องใช้ทรัพยากรอะไรในการขุดบ้าง

อ่าน ต่อฉบับหน้า

