



# ค่าเอาคอมพิวเตอร์ไปขุดอะไรกัน ?

อาจารย์อดิศักดิ์ เลื่อนิม

adisak@tni.ac.th

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีไทย-ญี่ปุ่น

**พัก** หลังนี้เรามักจะได้ยินคำว่า “นักขุด” หรือ “ขุด Bit” กันอยู่บ่อยๆ ถ้ากับคนที่ไม่ได้อยู่ในวงการ IT, การเงิน หรือการลงทุนมากนัก อาจจะต้องสงสัยไม่ได้ว่ามันคืออะไร วันนี้เราจะมาหาคำตอบกัน

โดยก่อนที่จะมารู้ว่า “นักขุด” หรือ “ขุด Bit” คืออะไร เราต้องเริ่มจากเข้าใจสกุลเงินดิจิทัล หรือ Crypto Currency เสียก่อนว่ามันเป็นสกุลเงินในรูปแบบใหม่ ที่มีความเป็นอิสระสูง และปราศจากการครอบงำจากหน่วยงานใดๆ โดยมีการทำงานในรูปแบบดิจิทัลที่จับต้องไม่ได้ โดยระบบออกแบบให้ทำการกระจายข้อมูลที่เข้ารหัส (Crypto คือ “การเข้ารหัส”) ออกเป็นส่วนย่อยๆ เข้าไปในเครือข่ายคอมพิวเตอร์เพื่อป้องกันไม่ให้ศูนย์กลางอยู่ที่ใดที่หนึ่ง (Decentralized) ซึ่งจะส่งผลให้ไม่มีใคร หรือกลุ่มใด สามารถควบคุมเงินสกุลนี้ได้ ซึ่งจะแตกต่างจากสกุลเงินปกติที่เราใช้อยู่ทุกวันนี้ ที่ถูกควบคุมได้ผ่านระบบธนาคารหรือแบงก์ชาติของแต่ละประเทศ

Bitcoin หรือ BTC เป็น Crypto Currency สกุลแรกของโลกที่เกิดขึ้นในปี 2009 ถูกพัฒนาขึ้นจากโปรแกรมเมอร์ที่ใช้นามแฝงว่า “Satoshi Nakamoto” ที่ได้ออกแบบให้ระบบ มีเงินจำกัดอยู่เพียง 21 ล้าน BTC และเงินสกุลนี้สามารถแยกย่อยได้ถึงทศนิยม 8 หลัก ดังนั้น เราจึงสามารถทำธุรกรรมกันด้วยเงินขนาด 0.00000001 BTC ได้ โดยปัจจุบันมีการทำธุรกรรมทางการเงินด้วย BTC ในหลายประเทศรวมทั้งประเทศไทยเราด้วย

ที่นี่เราลองมาเปรียบเทียบ BTC กับการทำธุรกรรมทางการเงินจริงๆ ที่เราใช้อยู่ เช่น ถ้าผมจะโอนเงินซื้อของออนไลน์จำนวน

1,000 บาท สิ่งที่จะเกิดขึ้น คือ ธนาคารต้องตรวจสอบว่าบัญชีของผมมีเงินถึง 1,000 บาทหรือไม่ โดยเมื่อโอนเงินแล้ว เงินในบัญชีผมต้องลดลง 1,000 บาท และเงินในบัญชีร้านค้าจะต้องเพิ่มขึ้น 1,000 บาท โดยธนาคารจะต้องบันทึกรายการธุรกรรมที่เกิดขึ้นทั้งหมด ลูกค้าสามารถเรียกดูข้อมูลย้อนหลังได้ ผมสามารถส่ง slip ยืนยันการโอนเงินไปให้ร้านค้าได้ อันนี้คือธุรกรรมทั่วไปที่เราทำกันอยู่

แต่ถ้าเทียบเป็นระบบของ BTC ทั้งหมด และร้านค้า จะต้องมีการบัญชี BTC ก่อน ซึ่งในทางปฏิบัติก็คือการใช้โปรแกรมที่เรียกว่า “bitcoin wallet” สำหรับสร้าง address เสมือนเป็นเลขที่บัญชีธนาคาร ซึ่งปัจจุบันจะมีหลายเว็บไซต์ที่ให้บริการด้านนี้อยู่ ข้อดีของการสร้างบัญชี BTC คือ คุณไม่ต้องกรอกข้อมูลส่วนตัวเหมือนกับการเปิดบัญชีธนาคารทั่วไป รวมถึงคุณจะได้เปิดบัญชีก็ได้

ดังนั้นถ้าผมจะโอนเงินให้ร้านค้า ผมก็แค่โอน BTC จาก address ของผม ไปยัง address ที่ร้านค้าให้ผมเท่านั้นเอง ... ทีนี้อาจจะมีคำถามตามมาว่า ผมจะไปหา BTC จากไหนมาเข้าบัญชีผมเพื่อไปซื้อของ คำตอบคือ ในปัจจุบันผมมีอยู่สองทางเลือกคือ

1. ทางเลือกแบบพื้นฐาน คือ เอาเงินสกุลปกตินี้แหละ ไปแลกเปลี่ยนเป็น BTC อาจใช้เงินบาทก็ได้ ซึ่งปัจจุบันก็มีหลายเว็บไซต์ทำหน้าที่เป็น Broker ที่จัดการเรื่องนี้ให้ ลองเข้า Google แล้วค้นหา Buy and sell bitcoins ดู (แต่ในความเป็นจริงแล้ว Broker ก็ไปรับซื้อจากกลุ่มคนที่เรียกว่า “นักขุด” อีกทีนี่เอามาขายต่อทำกำไร)

### Sell BTC

Bitcoins to sell:

You receive: **110,850 THB**

[Sell Coins](#)

Exchange BTC to THB rate:  
1 Bitcoin = 110,850.74 Thai Baht

---

### Buy BTC

Bitcoins to buy:

You pay: **116,076 THB**

[Buy Coins](#)

Exchange THB to BTC rate:  
1 Bitcoin = 116,076.00 Thai Baht

ข้อมูล อัตรา ซื้อ - ขาย BTC เทียบเงินบาท

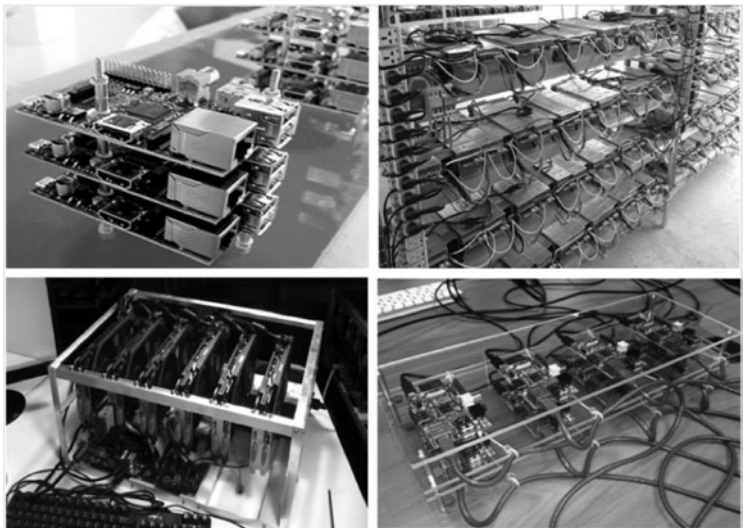
จากเว็บ <https://bitcoin.co.th> (08-08-17)

2. ทางเลือกนี้เกี่ยวข้องกับบทความนี้โดยตรง คือ ทำการ mining โดยการเอาคอมพิวเตอร์มาตั้งเพื่อทำงาน ถอดรหัส และได้ผลตอบแทนเป็น BTC โดยคนที่ทำงานในกลุ่มนี้เรียกกันว่า "นักขุด (Miners)" และกิจกรรมที่ทำงานแบบนี้ก็เรียกว่า "ขุด Bit"

โดยสาเหตุที่ระบบ BTC (ทั้งนี้รวมถึงเงินสกุลดิจิทัลอื่นๆ ด้วย) ต้องมีการ mining ก็เนื่องมาจากระบบ BTC ไม่ได้ทำธุรกรรมผ่านธนาคารเหมือนสกุลเงินปกติ คำถามสุดคลาสสิกคือ ... แล้วใครจะเป็นผู้ยืนยันความถูกต้องของบัญชี หรือใครจะเป็นผู้บันทึกธุรกรรมต่างๆ ที่เกิดขึ้นแทนธนาคาร ... คำตอบมันอยู่ที่เทคโนโลยีที่อยู่เบื้องหลัง BTC ที่เราเรียกกันว่า Block chain โดยเทคโนโลยีนี้เป็นรูปแบบการเก็บข้อมูลที่ทำให้ข้อมูลของแต่ละคนสามารถกระจายไปยังทุกๆ เครื่องในเครือข่ายได้ (ในที่นี้หมายถึงเครือข่ายนักขุดที่ใช้คอมพิวเตอร์มาประมวลผลถอดรหัส) โดยรูปแบบการเก็บข้อมูลจะเก็บต่อกัน เป็นบล็อก โดยการบันทึกข้อมูลในบล็อกใหม่ จะทำโดยเครื่องในเครือข่าย และจะทำได้ก็ต่อเมื่อเครือข่ายส่วนใหญ่ในระบบเห็นด้วยว่ามันถูกต้องเท่านั้น โดยเมื่อบล็อกข้อมูลได้ถูกบันทึกแล้ว จะมีความปลอดภัยสูงมาก ยากที่จะเข้าไปเปลี่ยนแปลง เพราะทุกเครื่องในเครือข่ายจะมีสำเนาของ Block chain เหมือนๆ กัน จึงสามารถตรวจสอบกันเองในระบบได้ ดังนั้นจึงยืนยันได้ว่าระบบนี้ปลอดภัยแน่นอน

โดยระบบ BTC ใช้ Block Chain ในการเก็บข้อมูลธุรกรรมทางการเงินในระบบ และไฮไลต์สำคัญอยู่ตรงที่ว่านักขุดในระบบจะต้องแข่งขันกันถอดรหัสสมการทางคณิตศาสตร์ที่ระบบสร้างมาให้ได้ก่อน ใครที่ถอดรหัสได้ก่อน จะได้สิทธิเป็นผู้บันทึกข้อมูลลงใน Block chain และจะได้รับรางวัลเป็น BTC ตอบแทนจากระบบอีกด้วย

เมื่อมีคำตอบเป็นแรงจูงใจแบบนี้แล้ว ทำให้มี "นักขุด" เข้าสู่ระบบอย่างมากมาย (ซึ่งก็เป็นไปตามโมเดลที่ผู้พัฒนาได้ออกแบบไว้ว่าระบบ BTC จะคงอยู่ได้จะต้องมีเครือข่ายนักขุดเป็น ผู้ทำงานแทนธนาคาร) โดยการขุดในทางปฏิบัติก็คือการรันซอฟต์แวร์เฉพาะที่ใช้ถอดรหัสสมการทางคณิตศาสตร์โดยใช้ความสามารถในการประมวลผลของเครื่อง เริ่มจากพื้นที่ ที่สุด ก็ใช้ CPU ของเครื่องคอมพิวเตอร์ที่เราใช้กันอยู่นี้แหละ ต่อมาค้นพบว่า การขุดก็ทำได้ๆ เราใช้เล่นเกมสมี CPU ในการประมวลผลที่แรงมาก จึงมีการนำ การ์ดจอมาใช้ในการขุด (ซึ่งส่งผลให้ที่ผ่านมา การขุดจอกับขาดตลาดไปเลยทีเดียว เพราะคนเหมาไปขุด Bit กัน) ถัดไปก็เริ่มมีการพัฒนาฮาร์ดแวร์เฉพาะสำหรับการขุดโดยตรง ออกมาขายกันอย่าง เป็นล่ำเป็นสัน โดยเน้นความเร็วในการประมวลผล และแก้ปัญหา ความร้อน และการกินไฟของการ์ดจอ และปัจจุบันได้มีการพัฒนารูปแบบการขุดมากขึ้น โดยการรวมกลุ่มกันของนักขุด ในรูปแบบที่ เรียกว่า pool โดยเมื่อได้ BTC มากก็จะนำมาแบ่งกันในกลุ่ม



ตัวอย่างการ "ขุด Bit" ด้วย Hardware แบบต่างๆ

ทั้งหมดนี้ถ้าจะคิดกันให้ถี่ถ้วน มันเริ่มจากสิ่งที่ไม่มีความหมายด้วยซ้ำ เงินสกุลดิจิทัลเป็นสิ่งที่ยังต้องไม่ได้ แต่สาเหตุที่มันมีการใช้งานกันในปัจจุบัน มีการขุดหาเงินสกุลดิจิทัล (ที่มีอีกมากมายหลายสกุล ไม่ใช่แค่ BTC) กันอย่างกว้างขวาง และมาไกลถึงทุกวันนี้ ทั้งหมดก็เพราะมนุษย์เราชอบมันเองว่ามันมีมูลค่า โดยส่วนตัวผู้เขียนเอง มีน้องๆ ที่รู้จักที่เข้าสู่วงการนักขุดตั้งแต่นยุคแรกๆ ที่ปัจจุบันก็ยังขุดอยู่ และก็มีอีกหลายคนเช่นกันที่เลิกแล้ว และขายอุปกรณ์ไปแล้ว เนื่องจากประเมินว่าไม่ได้คุ้มเสีย (ค่าไฟ, ค่าเสื่อมของอุปกรณ์) ดังนั้น ถ้าคิดจะทำอะไร อย่างแรกเลยคือต้องศึกษาหาความรู้ให้รอบด้านเสียก่อน อย่าคิดว่ามาขุด Bit แล้วจะรวยกันทุกคน เพราะขั้นที่ชื่อว่า coin หรือเหรียญแล้ว มันย่อมมีสองด้านเสมอ