



บิตคอยน์ ([Bitcoin](#)) เป็น [รูปแบบ](#) [ของ](#) [การ](#) [ชำระเงิน](#) [แบบ](#) [ดิจิทัล](#) [ที่](#) [ใช้](#) [ระบบ](#) [กระจาย](#) [อำนาจ](#) [โดย](#) [ไม่มี](#) [ศูนย์กลาง](#) [หรือ](#) [แม้แต่](#) [ผู้](#) [คุม](#) [ระบบ](#) [แม้แต่](#) [คนเดียว](#)

(cryptocurrency)

และเป็นระบบการชำระเงินที่ใช้กันทั่วโลก

บิตคอยน์เป็นสกุลเงินดิจิทัลแรกที่ใช้ระบบกระจายอำนาจ โดยไม่มี

[ศูนย์กลาง](#) [หรือ](#) [แม้แต่](#) [ผู้](#) [คุม](#) [ระบบ](#) [แม้แต่](#) [คนเดียว](#)

หรือแม้แต่ผู้คุมระบบแม้แต่คนเดียว

เครือข่ายเป็นแบบ

[การ](#) [ชำระเงิน](#) [แบบ](#) [ดิจิทัล](#) [ที่](#) [ใช้](#) [ระบบ](#) [กระจาย](#) [อำนาจ](#) [โดย](#) [ไม่มี](#) [ศูนย์กลาง](#) [หรือ](#) [แม้แต่](#) [ผู้](#) [คุม](#) [ระบบ](#) [แม้แต่](#) [คนเดียว](#)

และการซื้อขายเกิดขึ้นระหว่างจุดต่อเครือข่าย (

network node)

โดยตรง ผ่านการใช้

[การ](#) [ชำระเงิน](#) [แบบ](#) [ดิจิทัล](#) [ที่](#) [ใช้](#) [ระบบ](#) [กระจาย](#) [อำนาจ](#) [โดย](#) [ไม่มี](#) [ศูนย์กลาง](#) [หรือ](#) [แม้แต่](#) [ผู้](#) [คุม](#) [ระบบ](#) [แม้แต่](#) [คนเดียว](#)

และไม่มีสื่อกลาง

การซื้อขายเหล่านี้ถูกตรวจสอบโดยรายการเดินบัญชีแบบสาธารณะที่เรียกว่า

[การ](#) [ชำระเงิน](#) [แบบ](#) [ดิจิทัล](#) [ที่](#) [ใช้](#) [ระบบ](#) [กระจาย](#) [อำนาจ](#) [โดย](#) [ไม่มี](#) [ศูนย์กลาง](#) [หรือ](#) [แม้แต่](#) [ผู้](#) [คุม](#) [ระบบ](#) [แม้แต่](#) [คนเดียว](#)

บิตคอยน์ถูกพัฒนาโดยคนหรือกลุ่มคนภายใต้นามแฝง "ซาโตชิ นากาโมโตะ"

และถูกเผยแพร่ในรูปแบบซอฟต์แวร์โอเพนซอร์ซในปี พ.ศ.

2552

บิตคอยน์ถูกสร้างขึ้นใหม่ด้วย 'การขุด' (mining, การทำเหมือง) และสามารถแลกเปลี่ยนเป็นสกุลเงินอื่น สินค้าและบริการ ณ เดือนกุมภาพันธ์ พ.ศ. 2558 มีร้านค้ากว่า 100,000

มารู้จักบิตคอยน์

เขียนโดย นายบุญลือ

วันอาทิตย์ที่ 30 เมษายน 2017 เวลา 10:00 น. - แก้ไขล่าสุด วันพุธที่ 07 กุมภาพันธ์ 2018 เวลา 22:12 น.

ร้านยอมรับการจ่ายเงินด้วยบิตคอยน์

งานวิจัยจาก

[มหาวิทยาลัยเคมบริดจ์](#)

ประมาณว่าใน พ.ศ.

2560

มีผู้ใช้

[เงินตรา](#)

แบบ

[ดิจิทัล](#)

2.9

ถึง

5.8

ล้านคน โดยส่วนใหญ่แล้วใช้บิตคอยน์

หน่วยของบัญชีระบบบิตคอยน์คือ

บิตคอยน์

จนถึง พ.ศ.

2014

ชื่อที่ใช้ในการซื้อขาย (

ticker symbol)

ของบิตคอยน์ได้แก่

BTC

และ

XBT

โดยมีสัญลักษณ์

[ยูนิโคด](#)

หน่วยย่อยที่มักถูกใช้ได้แก่ มิลลิบิตคอยน์ (

mBTC)

และ ซาโตชิ ซึ่งเป็นชื่อที่ตั้งตามผู้สร้างบิตคอยน์ ซาโตชิเป็นหน่วยย่อยที่เล็กที่สุดแสดงจำนวน

0.00000001

บิตคอยน์ หรือ หนึ่งในร้อยล้านของบิตคอยน์

ส่วน

มิลลิบิตคอยน์

เท่ากับ

0.001

บิตคอยน์ หรือ หนึ่งในพันของบิตคอยน์ และยิ่งเท่ากับ

100,000

ซาโตชิ

มารู้จักบิตคอยน์

เขียนโดย นายบุญลือ

วันอาทิตย์ที่ 30 เมษายน 2017 เวลา 10:00 น. - แก้ไขล่าสุด วันพุธที่ 07 กุมภาพันธ์ 2018 เวลา 22:12 น.

ในวันที่

18

สิงหาคม พ.ศ.

2551

ชื่อโดเมน "

bitcoin.org"

ถูกตั้งขึ้น

↓

ในเดือนพฤศจิกายนปีเดียวกัน ลิงค์ไปยังเอกสารในหัวข้อ

บิตคอยน์:ระบบเงินอิเล็กทรอนิกส์แบบเพียร์ทูเพียร์

↓

เขียนโดย

[ซาโตชิ นากาโมโตะ](#)

ได้ถูกส่งไปยังกลุ่มรายชื่อของอีเมลของ

[วิทยาการเข้ารหัสลับ](#)

นากาโมโตะนำซอฟต์แวร์บิตคอยน์มาใช้เป็นโค้ดแบบโอเพนซอร์ซและเปิดตัวในเดือนมกราคม พ.ศ.

2552

ขณะนั้นจนถึงตอนนี้ตัวตนของนากาโมโตะยังไม่ถูกเปิดเผย

ในเดือนมกราคม พ.ศ. 2552 เครือข่ายบิตคอยน์ถือกำเนิดขึ้นหลัง ซาโตชิ นากาโมโตะ ใ้เมื่ชุดบล็อกแรกของเซนต์ที่เรียกว่าบล็อกกำเนิด ที่ให้รางวัลจำนวน 50 บิตคอยน์

หนึ่งในผู้สนับสนุน ผู้นำไปใช้ และผู้ร่วมพัฒนาบิตคอยน์คนแรก ๆ เป็นผู้รับการซื้อขายบิตคอยน์ครั้งแรก เขาเป็นโปรแกรมเมอร์ที่ชื่อว่า ฮาล ฟินนีย์ (Hal Finney) ฟินนีย์ดาวน์โหลดซอฟต์แวร์บิตคอยน์ในวันแรกที่เปิดตัว และได้รับ

10

บิตคอยน์จากนากาโมโตะในการซื้อขายบิตคอยน์ครั้งแรกของโลก

ผู้สนับสนุนแรกเริ่มคนอื่น ๆ ได้แก่

Wei Dai

ผู้สร้าง

b-money

และ

[Nick Szabo](#)

ผู้สร้าง

bit gold

ทั้งคู่ที่มาก่อนบิตคอยน์

ขอบคุณ youtube โดย mr. [Phongpech Jarubunyong](#)

ในช่วงแรก มีการประมาณว่านากาโมโตะได้ทำการขุดจำนวน 1 ล้านบิตคอยน์¹ ในพ.ศ. 2553 นากาโมโตะส่งต่อกุญแจเตือนเครือข่ายและการควบคุมที่เก็บโค้ดหลักบิตคอยน์ (Bitcoin Core code) ให้กับ [Gavin Andresen](#) ผู้ที่ต่อ

มากลายเป็นหัวหน้านักพัฒนาหลักของ

[#3617;ูลนิธิบิตคอยน์:](#)

(Bitcoin Foundation)

[\[32\]](#)

[\[33\]](#)

จากนั้นนากาโมโตะก็เลิกยุ่งเกี่ยวกับบิตคอยน์

จากนั้น

Andresen

ตั้งเป้าหมายว่าจะกระจายอำนาจการควบคุม และกล่าวว่า

"

หลังชาติขอยกออกไปและโยนโครงการมาบนไหล่ของฉัน สิ่งแรกที่ฉันทำคือการพยายามกระจายอำนาจ เพื่อที่โครงการจะไปต่อได้

แม้หากฉันโดนรถบัสชนก็ตาม"

มูลค่าของการแรกเปลี่ยนบิตคอยน์ครั้งแรกถูกต่อรองผ่านทางเว็บบอร์ดพูดคุยบิตคอยน์ โดยมีการซื้อขายครั้งหนึ่งที่ใช้ 10,000 BTC เพื่อซื้อพิกษาจำนวนสองถาดแบบ
บออมจาก [Papa John's](#)¹

เมื่อวันที่ 6 สิงหาคม พ.ศ. 2553 ช่องโหว่ครั้งใหญ่ในโพรโทคอลของบิตคอยน์ถูกพบ การซื้อขายไม่ได้ถูกตรวจสอบอย่างถูกต้องก่อนถูกใส่เข้าไปในบล็อกเชน

ทำให้ผู้ใช้สามารถเลี่ยงข้อจำกัดทางเศรษฐศาสตร์ของบิตคอยน์ และสร้างบิตคอยน์ขึ้นมาได้ในจำนวนไม่จำกัด

ในวันที่ 15 สิงหาคม

ช่องโหว่นี้ถูกใช้สร้างกว่า

184

ล้านบิตคอยน์ผ่านการซื้อขายหนึ่งครั้ง และส่งไปยังที่อยู่สองที่ในเครือข่าย การซื้อขายถูกพบภายในไม่กี่ชั่วโมง และถูกลบออกจากบันทึกหลังแก้ไข

[#3610;ัค:](#)

และอัปเดตหุ่นโพรโทคอลของบิตคอยน์

เมื่อวันที่ 1 สิงหาคม พ.ศ. 2560 ฮาร์ดฟอร์ค (hard fork) ของบิตคอยน์ถูกสร้างขึ้น เรียกว่า บิตคอยน์แคช (Bitcoin Cash) บิตคอยน์แคชมีข้อจำกัดของขนาดบล็อกที่ใหญ่ขึ้นและมีบล็อกเชนที่เหมือนกัน ณ เวลาฟอร์ค

บล็อกเชน

เป็น รายการบัญชีแบบสาธารณะที่บันทึกการซื้อขายบิตคอยน์

[\[40\]](#)

วิธีแก้ปัญหาแบบใหม่ทำสิ่งนี้โดยไม่ต้องพึ่งผู้มีอำนาจส่วนกลาง เพราะการรักษาความปลอดภัยเช่นทำโดยเครือข่ายของจุดต่อ (node)

ที่รันซอฟต์แวร์บิตคอยน์ซึ่งสื่อสารกัน

การซื้อขายในรูปแบบ ผู้จ่าย

X

ส่ง

Y

บิตคอยน์ ให้กับผู้รับ

Z

ถูกเผยแพร่ไปยังเครือข่ายนี้โดยใช้แอปพลิเคชันซอฟต์แวร์ที่มีอยู่

จุดต่อเครือข่ายสามารถตรวจสอบการซื้อขาย เพิ่มการซื้อขายไปบนรายการบัญชี จากนั้นเผยแพร่การเพิ่มรายการบัญชีเหล่านี้ไปยังจุดต่ออื่น ๆ บล็อกเชนเป็น

[ฐานข้อมูลแบบกระจาย](#)

(distributed database)

เพื่อการยืนยันอย่างอิสระของเซตของความเป็นเจ้าของบิตคอยน์ไม่ว่าจะจำนวนเท่าใด แต่ละจุดต่อเครือข่ายจัดเก็บสำเนาบล็อกเชนของตนเอง

ประมาณ

6

ครึ่งต่อชั่วโมง กลุ่มใหม่ของการซื้อขายที่ถูกยอมรับหรือที่เรียกว่าบล็อกถูกสร้างขึ้น เพิ่มเข้าไปในบล็อกเชน และเผยแพร่ไปยังจุดต่อทั้งหมดอย่างรวดเร็ว สิ่งนี้ทำให้ซอฟต์แวร์บิตคอยน์สามารถตัดสินใจว่าบิตคอยน์จำนวนที่กำหนดถูกใช้ และมีความสำคัญในการป้องกันการใช้จ่ายซ้ำ (

double-spending)

ในสภาพแวดล้อมที่ไม่มีส่วนกลางคอยควบคุม ในขณะที่รายการเดินบัญชีแบบดั้งเดิมบันทึกรายการซื้อขายของ

[ธนบัตร](#)

จริงหรือ

[ตั๋วสัญญาใช้เงิน](#)

บล็อกเชนเป็นที่เดียวที่บิตคอยน์สามารถมีอยู่ในรูปแบบของผลลัพธ์ที่ยังไม่ถูกใช้ในการซื้อขาย

logarithmic scale)

การซื้อขายถูกให้ความหมายด้วยภาษาบิตคอยน์ที่คล้ายฟอร์ธ (Forth) การซื้อขายประกอบไปด้วยข้อมูลเข้า และ ข้อมูลออก เมื่อผู้ใช้ส่งบิตคอยน์ ผู้ใช้กำหนดที่อยู่และจำนวนบิตคอยน์ที่จะส่งไปยังที่อยู่นั้นในข้อมูลออก เพื่อป้องกันการใช้ซ้ำซ้อน ข้อมูลเข้าแต่ละข้อมูลต้องอ้างอิงกลับไปยังข้อมูลออกอันก่อนที่ยังไม่ได้ใช้ในบล็อกเชน

การใช้ข้อมูลเข้าหลายข้อมูลเปรียบเสมือนการใช้เหรียญหลายเหรียญในการซื้อขายด้วยเงินสด ในเมื่อการซื้อขายสามารถมีข้อมูลออกหลายข้อมูล ผู้ใช้สามารถส่งบิตคอยน์ให้กับหลายผู้รับในการซื้อขายหนึ่งครั้ง ผลรวมของข้อมูลเข้า (จำนวนเหรียญที่ใช้จ่าย) สามารถมีจำนวนมากกว่าจำนวนจ่ายทั้งหมด เช่นเดียวกับการซื้อขายด้วยเงินสด ในกรณีนี้ ข้อมูลออกเสริมถูกใช้เพื่อทอนให้กับผู้จ่าย

จำนวนชาติที่ถูกบ่อนเข้าและไม่ถูกบันทึกสำหรับการซื้อขายออกกลายเป็นค่าธรรมเนียมการซื้อขาย

การขุด (

mining)

เป็นบริการบันทึกข้อมูลผ่านการใช้

[พลังในการคำนวนผล](#)

(processing power)

ของคอมพิวเตอร์

ผู้ขุด (

miner)

ช่วยทำให้บล็อกเชนมีความสม่ำเสมอ สมบูรณ์ และเปลี่ยนแปลงไม่ได้ โดยการตรวจสอบซ้ำ ๆ

และเก็บบันทึกการซื้อขายใหม่ที่ถูกเผยแพร่ไปยังกลุ่มการซื้อขายใหม่ที่เรียกว่า

บล็อก

แต่ละบล็อกประกอบไปด้วย

[การเข้ารหัสแบบแฮช](#)

(cryptographic hash)

หรือการเข้ารหัสทางเดียว ของบล็อกก่อนหน้า

โดยการใช้ขั้นตอนวิธีแฮช

[SHA-256](#)

[\[43\]](#)

[:ch.7](#)

ซึ่งเชื่อมต่อกับบล็อกก่อนหน้า

เป็นจุดกำเนิดของชื่อ

[บล็อกเชน](#)

บล็อกใหม่ต้องมีสิ่งทีเรียกว่า การพิสูจน์งาน (Proof-of-work) จึงจะได้รับการยอมรับจากระบบ การพิสูจน์งานต้องการให้ผู้ขุดหาตัวเลขที่เรียกว่า nonce ที่ให้ผลลัพธ์จำนวนน้อยกว่าเป้าหมายความยากของระบบเมื่อถูกเข้ารหัสแบบแฮชด้วย

nonce

[\[43\]](#)

:ch. 8

การพิสูจน์นี้ง่ายที่สุดต่อได้ก็ตามที่เป็นส่วนหนึ่งของเครือข่ายจะทำการตรวจสอบ ทว่ากินเวลาอย่างมากหากจะสร้างขึ้นเอง ผู้ชุดต้องลงจำนวน
nounce

หลายจำนวนเพื่อบรรลุเป้าหมายความยาก โดยมักเริ่มทดสอบจากค่า

0, 1, 2, 3, ...

ตามลำดับ

ทุก ๆ 2,016 บล็อก (ประมาณ 14 วัน หากใช้เวลา 10 นาทีต่อบล็อก) เป้าหมายความยากถูกปรับตามสมรรถนะใหม่ของระบบ

โดยมีเป้าหมายที่จะคงเวลาเฉลี่ยระหว่างบล็อกใหม่ไว้ที่

10 นาที

วิธีนี้ทำให้ระบบปรับตัวเข้ากับพลังการขุดของเครือข่ายอย่างอัตโนมัติ

ระหว่างวันที่ 1 มีนาคม พ.ศ. 2557 จนถึง 1 มีนาคม พ.ศ. 2558 จำนวนเฉลี่ยของnounce ที่นักขุดต้องทดลองเพื่อสร้างบล็อกใหม่เพิ่มขึ้นจาก 16.4×10^{18} เป็น 200.5×10^{18}

ระบบการพิสูจน์งานคู่กับการต่อกันของบล็อกทำให้การเปลี่ยนแปลงของบล็อกเชนเป็นไปได้ยากมาก เพราะการที่ผู้โจมตีจะทำให้บล็อกหนึ่งได้รับการยอมรับ

จำเป็นต้องเปลี่ยนแปลงบล็อกต่อมาที่เชื่อมกันทั้งหมด เมื่อเวลาผ่านไปความยากในการเปลี่ยนแปลงบล็อกเพิ่มขึ้น

ด้วยความที่บล็อกใหม่ถูกขุดตลอดเวลาทำให้จำนวนบล็อกที่ตามมาเพิ่มขึ้นไปด้วย

ผู้ชุดที่หาบล็อกใหม่สำเร็จได้

รางวัลเป็นบิตคอยน์ที่ถูกสร้างขึ้นและค่าธรรมเนียมการซื้อขาย

ณ วันที่

9

กรกฎาคม พ.ศ.

2559

รางวัลอยู่ที่จำนวน

12.5

บิตคอยน์ที่ถูกสร้างใหม่ต่อบล็อกที่ถูกเพิ่มไปยังบล็อกเชน เพื่อขอรับรางวัล การซื้อขายพิเศษที่เรียกว่า

คอยน์เบส

ถูกรวมเข้ากับการจ่ายที่ถูกดำเนินการ

บิตคอยน์ที่มีอยู่ทั้งหมดถูกสร้างด้วยการซื้อขายแบบคอยน์เบสนี้

โพรโทคอลของบิตคอยน์ระบุว่ารางวัลสำหรับการเพิ่มบล็อกจะถูกลดเหลือครึ่งหนึ่งทุก ๆ 210,000 บล็อก (ประมาณทุก ๆ 4 ปี)

จนในที่สุดรางวัลจะถูกลดลงเป็นศูนย์ โดยมีจำนวนสูงสุดอยู่ที่

21

ล้านบิตคอยน์

ประมาณปีพ.ศ.

มารู้จักบิตคอยน์

เขียนโดย นายบุญลือ

วันอาทิตย์ที่ 30 เมษายน 2017 เวลา 10:00 น. - แก้ไขล่าสุด วันพุธที่ 07 กุมภาพันธ์ 2018 เวลา 22:12 น.

2683

จากนั้นรางวัลของการบันทึกจะเหลือเพียงค่าธรรมเนียมเท่านั้น

กล่าวคือ นากาโมโตะ ผู้สร้างบิตคอยน์ ตั้ง [#3609;#3650;#3618;#3610;#3634;#3618;#3585;#3634;#3619;#3648;#3591;#3636;#3609;](#)

บนฐานของ [#3588;#3623;#3634;#3617;#3586;#3634;#3604;#3649;#3588;#3621;#3609;#3611;#3619;#3632;#3604;#3636;#3625;#3600;#3660;](#) (artificial scarcity) และทำให้

บิตคอยน์ถูกจำกัดอยู่ที่จำนวน

21

ล้านบิตคอยน์ตั้งแต่แรก จำนวนทั้งหมดจะถูกเผยแพร่ทุก ๆ สิบนาทีและอัตราการสร้างจะลดลงครึ่งหนึ่งทุก ๆ สี่ปีจนบิตคอยน์ทั้งหมดอยู่ในระบบ

-

ขอบคุณ

wikipedia.