Bitcoin: สกุลเงินของการเข้ารหัสลับที่น่าจับตามอง

Bitcoin: The Encryption Currency

อัญชณา เหมือนคิด [1], ธนพล พุกเส็ง[2], ระดม เจือจันทร์[3], ศิรปัฐช์ บุญครอง [4]

Anchana Muankid[1], Thanaphon Phukseng [2], Radom Juajan [3], Sirapat Boonkrong [4]

Received: 20 January 2014 ; Accepted: 29 March 2014

บทคัดย่อ

บทความนี้กล่าวถึงสกุลเงินดิจิตอลแบบ peer-to-peer ซึ่งสามารถเปิดบัญชีใหม่ได้ด้วยตนเองโดยการสร้างกุญแจสาธารณะซึ่งเปรียบเสมือนเลขที่บัญชี และกุญแจส่วนตัวที่ใช้ในการยืนยันข้อความ การยืนยันความถูกต้องของธุรกรรมและการป้องกันปัญหาการคัดลอกไฟล์เพื่อจ่ายเงินซ้ำซ้อน (Double-spending) ของ Bitcoin นั้น ได้นำการเข้ารหัสแบบกุญแจสาธารณะ (Public-Key Cryptography) มาประยุกต์ใช้การพัฒนา Bitcoin จึงถือเป็นการปฏิวัติครั้งใหญ่ เนื่องจากเป็นครั้งแรกที่ปัญหา Double-spending ถูกแก้ไขโดยไม่จำเป็นต้องมีบุคคลที่สามเข้ามาเกี่ยวข้อง โดยผู้ใช้ระบบจะมีบัญชีกระจายผ่านเครือข่าย peer-to-peer ทุกรายการธุรกรรมที่ปรากฏในระบบของ Bitcoin จะถูกบันทึกเป็นสาธารณะที่ผู้ใช้ทุกคนสามารถตรวจสอบได้ ข้อดีของ Bitcoin คือ มีการทำธุรกรรมที่ราคาถูกและรวดเร็วกว่าการชำระเงินปกติ ในการใช้งานจริง มีผู้ให้บริการหลายรายที่รับชำระเงินผ่าน Bitcoin เช่น WordPress.com, Namecheapและ Zynga เป็นต้น แต่ก็มีผู้ใช้ Bitcoin ในการซื้อสินค้าและบริการที่ผิดกฎหมายได้เช่นกัน ตัวอย่างเช่น กรณีของตลาดมืดออนไลน์ ‘Silk Road’ ที่ซ่อนตัวอยู่บนเครือข่าย Tor อย่างไรก็ดี ปัญหาและความเสี่ยงในด้านความปลอดภัย และความผันผวนอย่างมากของมูลค่าจากการใช้ Bitcoin ก็ยังสามารถพบได้ นอกจากนี้การขาดความยอมรับในด้านกฎหมายเป็นอีกปัจจัยสำคัญที่ผู้ที่สนใจควรพิจารณาอย่างรอบคอบก่อนการใช้เงินเสมือนอย่าง Bitcoin

คำสำคัญ: บิทคอยน์ เงินดิจิตอล การเข้ารหัส

Abstract

This article discusses peer-to-peer digital currency covering public keys, which are an account number, and private keys which are used to confirm messages. Public-Key Cryptography is used to verity transactions and prevents the double-spending problem of Bitcoin. Thus, Bitcoin has solved the Double-spending problem without third party involvement. User accounts are distributed through peer-to-peer networks, all Bitcoin transactions are recorded publicly which can be audited by anyone. The advantages of Bitcoin payments are speed and no extra fees as with normal payment options. There are now many providers that accept Bitcoin payment such as WordPress.com, Namecheap, Zynga etc. But some Bitcoin users also purchase illegal services, for example, in the case of the online dark market ‘Silk Road’ which is hidden in the Tor network of the internet. The security and volume of fluctuations are a few of problems for Bitcoin users. In addition, the lack of legal recognition is an important factor that should considered before using Bitcoin.

Keywords: bitcoin, digital-currency, cryptography

[1,2,3] *นิสิตปริญญาเอก, คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ประเทศไทย. [4]ผู้ช่วยศาสตราจารย์, คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ประเทศไทย. E-mail: gabbygift@gmail.com*

[1,2,3] *Doctoral degree student Faculty of Information Technology, King Mongkut's University of Technology, North Bangkok, Thailand. [4]Assistant Professor, Faculty of Information Technology, King Mongkut's University of Technology, North Bangkok, Thailand. E-mail: gabbygift@gmail.com*

* *Corresponding author: E-mail: gabbygift@gmail.com*

บทนำ

เงินเป็นสื่อกลางในการทำธุรกรรมซื้อขายแลกเปลี่ยนสินค้า ถูกควบคุมโดยธนาคาร และสถาบันการเงินระหว่างประเทศ ซึ่งมีอำนาจในการกำหนดค่าเงินของตนเองด้วยกระบวนการต่าง ๆ นอกจากนี้ยังมีอำนาจในการติดตามและตรวจสอบการเงินของผู้ใช้อีกด้วย จึงมีแนวคิดสร้างระบบการเงินที่ควบคุมด้วยเทคโนโลยีแทน Satoshi Nakamoto บุคคลลึกลับที่อ้างว่ามาจากประเทศญี่ปุ่นเริ่มพัฒนา Bitcoin ในปี ค.ศ. 2007 และนำมาใช้จริงในปี ค.ศ. 2009 เชื่อกันว่าชื่อ Satoshi ถูกสร้างขึ้นเพื่อโครงการนี้โดยเฉพาะ เมื่อพิจารณาจากความเชี่ยวชาญในการเข้ารหัสที่สูงมากแต่กลับไม่มีชื่อปรากฏในวงการวิชาการเข้ารหัส

โดเมนหลักของโครงการคือ BitCoin.org นั้นถูกจดทะเบียนกับบริษัทรับจดทะเบียนแบบปกปิดตัวตน ก่อนจะโอนให้กับ MarttiMalmi นักพัฒนาหลักของโครงการ[1] Bitcoin เป็นสกุลเงินดิจิตอลแบบ peer-to-peer สามารถเปิดบัญชีใหม่ได้ด้วยตนเองโดยการสร้างกุญแจสาธารณะซึ่งเปรียบเสมือนเลขที่บัญชี และกุญแจส่วนตัวที่ใช้ในการยืนยันข้อความ สามารถตรวจสอบจำนวนเงินของทุกบัญชีได้ และทุกครั้งที่มีการทำธุรกรรม ข้อมูลจะถูกกระจายไปทั่วเครือข่าย[2] สิ่งที่ทำให้ Bitcoin ได้รับความนิยมอย่างมากเนื่องจาก เป็นระบบการเงินดิจิตอลแบบไร้ศูนย์กลาง (Decentralized) อย่างสมบูรณ์รายแรกในโลก[3]

ก่อนที่จะมี Bitcoin การทำธุรกรรมทางการเงินออนไลน์จะต้องมีบุคคลที่สามเข้ามาเกี่ยวข้อง เช่น หาก Alice ต้องการโอนเงิน $100 ให้ Bob ผ่านทางอินเทอร์เน็ต Alice จำเป็นที่จะต้องโอนไปยังบุคคลที่สาม เช่น Pay Pal หรือ Master Card โดยที่บุคคลเหล่านั้นจะเก็บข้อมูลยอดเงินคงเหลือของผู้ถือบัญชี เมื่อ Alice ส่ง $100 ให้ Bob นั่นหมายถึง Pay Pal จะตัดยอดเงินจากบัญชีของ Alice และเพิ่มยอดเงินดังกล่าวในบัญชีของ Bob [3] หากไม่มีคนกลาง เงินดิจิตอลอาจถูกจ่ายซ้ำซ้อนได้ หากลองเปรียบเทียบเงินดิจิตอลเป็นเพียงไฟล์คอมพิวเตอร์หนึ่งไฟล์ Alice ส่ง $100 ให้ Bob โดยการแนบไฟล์เงินดังกล่าวไปกับข้อความคล้ายกับการส่งอีเมล์ ไฟล์ที่แนบไปจะไม่ถูกลบออกจากคอมพิวเตอร์ ดังนั้น Alice สามารถคัดลอกไฟล์เงินดังกล่าวส่งไปให้คนอื่น ๆ ได้อีก ปัญหานี้เรียกว่า “Double-spending” [4]

การพัฒนา Bitcoin จึงถือเป็นการปฏิวัติครั้งใหญ่ เนื่องจากเป็นครั้งแรกที่ปัญหา Double-spending ถูกแก้ไขโดยไม่จำเป็นต้องมีบุคคลที่สามเข้ามาเกี่ยวข้อง ซึ่งวิธีที่ใช้แก้ไขปัญหาดังกล่าว คือ ผู้ใช้ระบบจะมีบัญชีกระจายผ่านเครือข่าย peer-to-peer ทุกรายการธุรกรรมที่ปรากฏในระบบของ Bitcoin จะถูกบันทึกเป็นสาธารณะที่ผู้ใช้ทุกคนสามารถตรวจสอบได้[3]

บทความวิจัยชิ้นนี้มีวัตถุประสงค์เพื่อนำเสนอข้อมูลเกี่ยวกับการทำงานของ Bitcoin การใช้งานในด้านต่าง ๆ รวมถึงปัญหาในด้านความปลอดภัยของ Bitcoin

การทำงานของ Bitcoin

การยืนยันความถูกต้องของธุรกรรมและการป้องกันปัญหา Double-spending ของ Bitcoin นั้น ได้นำการเข้ารหัสแบบกุญแจสาธารณะ (Public-Key Cryptography) มาประยุกต์ใช้ การเข้ารหัสแบบกุญแจสาธารณะนั้น ผู้ใช้แต่ละคนต้องสร้างกุญแจขึ้นมาสองตัว ได้แก่ กุญแจส่วนตัว (Private Key) ซึ่งต้องเก็บไว้เป็นความลับ และ กุญแจสาธารณะ (Public Key) ซึ่งสามารถประกาศให้ผู้อื่นทราบได้ [5] การเริ่มต้นการใช้งาน Bitcoin เพื่อเป็นตัวกลางในการแลกเปลี่ยนสินค้าและบริการ จำเป็นต้องมีบัญชีของผู้ใช้งาน โดยใช้ซอฟต์แวร์สร้าง “Bitcoin Wallet” สำหรับเก็บรักษา Bitcoin ซึ่งสามารถติดตั้ง Bitcoin Wallet บนคอมพิวเตอร์ และอุปกรณ์พกพาต่าง ๆ หรือสามารถฝากไว้กับผู้ให้บริการบนอินเทอร์เน็ตได้ Wallet แต่ละใบจะมีที่อยู่เป็นตัวเลขผสมอักษรยาว 34 ตัวอักษร ซึ่งได้มาจากกุญแจสาธารณะ ตัวอย่างที่อยู่ของ Wallet แสดงดัง Figure 1 Bitcoin Wallet จะเก็บยอดเงินคงเหลือ ประวัติการทำธุรกรรมเบื้องต้น และที่อยู่ของผู้ที่ทำธุรกรรมด้วย แต่จะไม่มีการเปิดเผยข้อมูลของผู้ใช้ว่าเป็นใคร และไม่จำเป็นต้องแสดงตัวตนในการใช้บริการ[6]

Figure 1 Bitcoin Wallet Address [6]

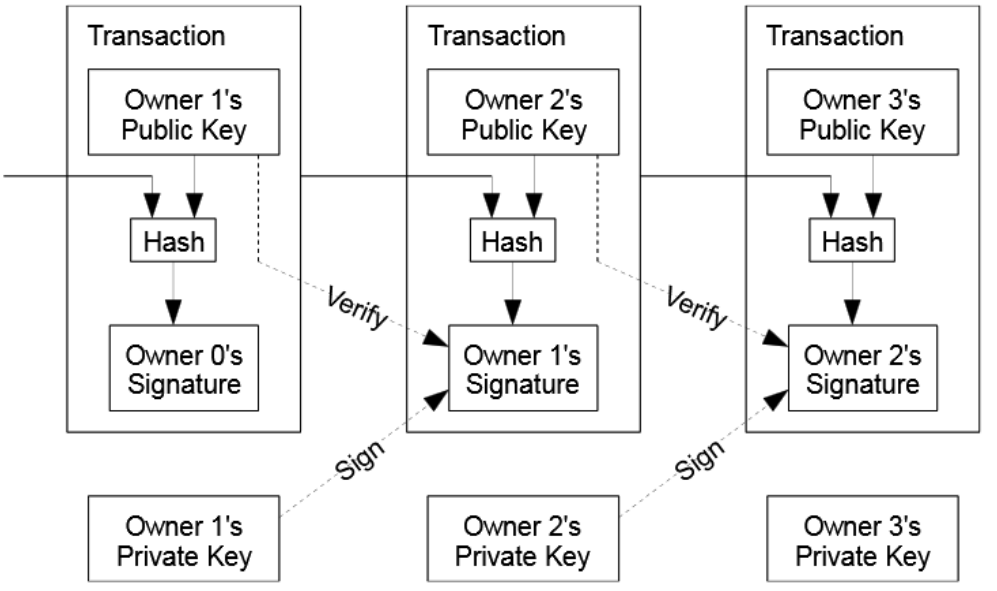

Figure 2 Transaction process[7]

การทำธุรกรรมสามารถทำได้โดยระบบจะส่งข้อมูลของธุรกรรม พร้อมลายเซ็นดิจิตอลเฉพาะบุคคล (Signature) ซึ่งสัมพันธ์กับที่อยู่ของ Wallet ของผู้ส่งรายการธุรกรรมไปยังผู้ใช้คนอื่น ๆ ภายในโครงข่ายของผู้ใช้ Bitcoin ซึ่งจะทำหน้าที่ตรวจสอบลายเซ็นของผู้ส่งรายการก่อนที่จะมีการอนุมัติการทำรายการในระยะเวลาต่อมา

กระบวนการตรวจสอบธุรกรรมของ Bitcoin เป็นกระบวนการที่สำคัญที่สุดเมื่อผู้ใช้กำหนดมูลค่า Bitcoin ที่ต้องการโอน ต่อท้ายด้วยที่อยู่ของผู้รับซึ่งนั่นคือกุญแจสาธารณะของผู้รับ จากนั้นโปรแกรมคำนวณหาค่า Hash แบบ SHA256 ของการทำธุรกรรมรวมกับ Time-stamp ได้เป็น Block ขั้นตอนการทำธุรกรรมแสดงดัง Figure 2 การยืนยันการโอนแต่ละ Block จะต้องปรับค่า nonce ที่ใช้เติมเพื่อให้ค่า Hash มีคุณสมบัติตรงตามค่าเป้าหมายที่กำหนด[7] แต่ละ Block ของ Bitcoin จะอ้างถึง Block ก่อนหน้าเสมอ ส่งผลให้แต่ละ Block อ้างถึงกันเป็นลูกโซ่ไปข้างหน้าทางเดียว เรียกว่า “Block Chain” การคำนวณค่า Block ปัจจุบันจึงเป็นการยืนยันความถูกต้องของ Block ก่อนหน้า โดยปกติแล้ว ซอฟต์แวร์ Bitcoin Wallet จะแจ้งผู้ใช้ว่าการโอนเงินได้รับการยืนยันต่อเมื่อ Block ที่บันทึกการโอนเงินถูกอ้างถึงไปอีก 6 Block ข้างหน้า[1] การเข้ารหัสแบบกุญแจสาธารณะนั้นจึงทำให้มั่นใจได้ว่าการโอนเงินในระบบ Bitcoin นั้นสามารถทำได้อย่างปลอดภัยและป้องกันปัญหา Double-spending ได้

ปัจจุบันการคำนวณ Block ใหม่ใช้เวลา 5-10 นาที ในช่วงแรกโปรแกรม Bitcoin Wallet จะเปิดให้ทุกเครื่องช่วยกันคำนวณ Block ไปพร้อม ๆ กัน แต่เนื่องจากการคำนวณยากขึ้นเรื่อย ๆ จนคอมพิวเตอร์ธรรมดาไม่สามารถคำนวณได้ทัน ช่วงหลังจึงมีการรวมกลุ่มเพื่อเร่งคำนวณค่า Hash ให้เร็วขึ้น บางกลุ่มเปิดรับสมาชิกโดยมีสัญญาว่าจะแบ่งเงินให้ตามสัดส่วนที่คำนวณได้ เรียกว่า Mining Pool[1] ซึ่งกลไกการรักษามูลค่าของ Bitcoin นั้นมี Protocol ที่กำหนดไว้ว่า จำนวน Bitcoin ที่ถูกสร้างขึ้นจะมีจำนวนทั้งหมดไม่เกิน 21 ล้านหน่วย ซึ่งปัจจุบันถูกพบแล้ว 12 ล้านหน่วยในระบบ [6]

การใช้งาน Bitcoin

Bitcoin ยังคงเป็นเงินสกุลใหม่และมีความผันผวนมาก จึงยังไม่ได้รับการยอมรับจากผู้ประกอบการค้าหลาย ๆ แห่ง ข้อดีของ Bitcoin คือ มีการทำธุรกรรมที่ราคาถูก เนื่องจากไม่มีบุคคลที่สามเข้ามาเกี่ยวข้อง การทำธุรกรรมของ Bitcoin จึงมีราคาถูกและรวดเร็วกว่าการชำระเงินปกติ Bitcoin ทำให้สามารถเข้าถึงบริการทางการเงินขั้นพื้นฐาน[3] และยังกระตุ้นให้เกิดนวัตกรรมทางด้านการเงิน เนื่องจาก Protocol ของ Bitcoin ประกอบด้วยข้อมูลเกี่ยวกับตัวเลขทางการเงินและบริการที่ได้รับอนุญาต ซึ่งทำให้นักพัฒนาโปรแกรมสามารถพัฒนาต่อได้ไม่ยาก

การใช้ Bitcoin ชำระค่าสินค้าและบริการทั่วไป

ในการใช้งานจริง มีผู้ให้บริการหลายรายที่รับชำระเงินผ่าน Bitcoin ในเดือนพฤศจิกายน ปี ค.ศ.2012 Word-Press.com ผู้ให้บริการเว็บบล็อกรายใหญ่ประกาศให้บริการรับชำระผ่าน Bitcoin เหตุผลสำคัญของ WordPress ที่รับชำระค่าบริการผ่าน Bitcoin เนื่องจาก การชำระเงินผ่าน PayPal และบัตรเครดิตยังมีข้อจำกัดในหลายประเทศ [8] บริษัทรับจดโดเมนรายใหญ่ Namecheap ระบุว่ามีผู้ใช้บริการหลายรายที่เสนอให้ Namecheap รับชำระค่าบริการผ่าน Bitcoin ซึ่งทางบริษัทก็ได้รับข้อเสนอดังกล่าวและประกาศรับชำระผ่านทาง Bitcoin ในเดือนมีนาคม ปี ค.ศ. 2013 [9]หลังจากนั้น การใช้ Bitcoin ในการซื้อสินค้าและบริการต่าง ๆ ได้รับความนิยมมากขึ้น ในเดือนตุลาคม ปี ค.ศ. 2013 แคนาดาได้เปิดตัวตู้ ATM Bitcoin ตู้แรกของโลกที่ร้านกาแฟแห่งหนึ่งในนครแวนคูเวอร์ [10] โดยสามารถนำ Bitcoin แลกเป็นเงินสด หรือเงินสดแลกเป็น Bitcoin ได้ ล่าสุดเมื่อเดือน มกราคม ปี ค.ศ. 2014 Zynga บริษัทยักษ์ใหญ่ด้านเกมออนไลน์บน Facebook ประกาศทดสอบระบบซื้อของในเกมส์ด้วย Bitcoin โดยมี BitPay ซึ่งเป็นบริการรับชำระผ่าน Bitcoin ร่วมพัฒนาระบบด้วย [11]

ล่าสุด เมื่อวันที่ 28 กุมภาพันธ์ 2557 สำนักข่าว Reuter รายงานว่า Mt.Gox ซึ่งเป็นตลาดซื้อขาย Bitcoin รายใหญ่ที่สุดและได้รับความนิยมมากที่สุดได้ยื่นเอกสารต่อศาลโตเกียว ประเทศญี่ปุ่นเพื่อขอล้มละลาย ผู้บริหาร Mt.Gox ยอมรับว่า เกิดความผิดพลาดในระบบซื้อขาย และ Bitcoin ของลูกค้าทั้งหมดน่าจะสูญหาย คิดเป็นจำนวนเงิน 63.67 ล้านดอลลาร์ มีผู้เสียหายราว 127,000 คน ส่งผลให้ค่าเงินมีความผันผวนมากขึ้น[13] ซึ่งรายละเอียดจะกล่าวในหัวข้อปัญหาด้านความปลอดภัย

Figure 3 The first Bitcoin ATM[12]

สำหรับในประเทศไทย การแลก Bitcoin เป็นเงินบาท ยังไม่มีกฎหมายรองรับ เนื่องจากผู้รับแลก Bitcoin ในไทยไม่ได้เป็นผู้ประกอบการภายใต้ พ.ร.บ. ควบคุมการแลกเปลี่ยนเงิน พ.ศ. 2485 นอกจากนี้ กฎหมายไทยยังระบุว่า ในการซื้อ-ขายสินค้าในราชอาณาจักรไทย จำต้องใช้เงินบาทเป็นสื่อกลางในการชำระหนี้ตามกฎหมาย ทำให้ผู้ซื้อต้องรับความเสี่ยงจากความผิดพลาดหรือปัญหาที่เกิดขึ้นที่เกี่ยวข้องกับระบบ Bitcoin ด้วยตนเอง [6]

การใช้ Bitcoin ในทางผิดกฎหมาย

เช่นเดียวกับเงินทั่วไป Bitcoin สามารถใช้ในการซื้อสินค้าและบริการที่ถูกกฎหมาย และสามารถใช้ในการซื้อสินค้าและบริการที่ผิดกฎหมายได้เช่นกัน ตัวอย่างเช่น กรณีของตลาดมืดออนไลน์ ‘Silk Road’ ที่ซ่อนตัวอยู่บนเครือข่าย Tor [3]

เครือข่าย Tor เป็นระบบที่ออกแบบมาเพื่อช่วยในการออนไลน์แบบไร้ตัวตน ซึ่งอาศัยการเข้ารหัสข้อมูลมาช่วยในการส่งข้อความระหว่างคอมพิวเตอร์แต่ละเครื่อง คอมพิวเตอร์ที่ได้รับข้อความจะถอดรหัสข้อความเพื่อดูว่าตนเองต้องส่งข้อความดังกล่าวต่อไปยังคอมพิวเตอร์เครื่องใดในเครือข่าย ดังนั้น การติดตามหรือตรวจสอบหาผู้ส่งที่แท้จริงจึงทำได้ยาก[14]

Silk Road ใช้ประโยชน์ของเครือข่าย Tor และ Bitcoin ในการสร้างตลาดซื้อขายยาเสพติดที่ได้รับความนิยมมาก ถึงแม้ผู้ดูแล Silk Road จะไม่อนุญาตให้แลกเปลี่ยนสินค้าที่ได้มาจากการฉ้อโกง เช่น ข้อมูลของบัตรเครดิตที่ขโมยมา หรือภาพอนาจารเด็ก แต่มีการอนุญาตให้ขายสินค้าผิดกฎหมายได้ เช่น เอกสารปลอม ยาเสพติด เป็นต้น[3] งานวิจัยชิ้นหนึ่ง ผู้วิจัยศึกษามูลค่าซื้อขายในเว็บ Silk Road พบว่า มียอดขายสูงถึง 1.2 ล้านดอลลาร์สหรัฐต่อเดือน[15]หลังจากที่ผู้ดูแล Silk Road เพิ่งให้สัมภาษณ์ผ่านเครือข่าย Tor ไม่นาน Silk Road ได้ถูก

ปิดลง เนื่องจาก FBI สามารถจับกุมผู้ดูแล Silk Road ได้ ในข้อหาการสนับสนุนการค้ายาเสพติด แฮคข้อมูลคอมพิวเตอร์ และฟอกเงิน โดย FBI ไม่ได้เปิดเผยว่าสามารถสืบหา server ของ Silk Road ที่ซ่อนตัวอยู่บนเครือข่าย Tor ได้อย่างไร[16]

งานวิจัยเกี่ยวกับธุรกรรมของ Bitcoin ชิ้นล่าสุด นักวิจัยได้วิเคราะห์การโอนเงินก้อนใหญ่ในระบบ Bitcoin พบว่า เงินก้อนใหญ่ทั้งหมดมีความสัมพันธ์กับเงินก้อนหนึ่งที่ถูกโอนในช่วงปี 2010 โดยเงินก้อนแรกที่โอนมีมูลค่า 90,000 BTC หลังจากนั้นพบว่า มีการโอนเงินก้อนใหญ่ที่สัมพันธ์กับการโอนเงินครั้งแรกอีกหลายครั้ง[17] และยังพบความเชื่อมโยงอันน่าประหลาดใจระหว่างผู้สร้าง Bitcoin และ ผู้ดูแลตลาดมืด Silk Road นักวิจัยค้นพบความเคลื่อนไหวของเงินจากบัญชีที่ถูกสร้างขึ้นเมื่อวันที่ 16 มกราคม 2009 ซึ่งเป็นเวลา 1 สัปดาห์หลังจากเงิน Bitcoin ถูกสร้างขึ้นครั้งแรก โดยมีการโอนเงินจำนวน 1,000 BTC สู่บัญชีของผู้ดูแลตลาดมืด Silk Roadซึ่งผู้วิจัยอธิบายว่า การเคลื่อนไหวลักษณะนี้อาจเป็นการเคลื่อนไหวครั้งใหญ่บนตลาดมืด Silk Road ซึ่งเป็นสิ่งที่น่าพิจารณาเป็นอย่างยิ่ง[18]

นอกจากการใช้ Bitcoin ในการซื้อขายสินค้าและบริการในตลาดมืดแล้ว ยังพบว่า มีการใช้ Bitcoin ในเว็บพนันออนไลน์ขนาดใหญ่ที่ชื่อ Satoshi Dice[19] และใช้ในการซื้อขายสื่อลามกในเว็บ Porn.com อีกด้วย[20]

ปัญหาด้านความปลอดภัย

ความท้าทายในด้านความปลอดภัยจะมุ่งเน้นไปที่บริการ Wallet และการแลกเปลี่ยน Bitcoin ซึ่ง Protocol Bitcoin ได้ถูกทดสอบความเสี่ยงในด้านความปลอดภัยและการถูกโจมตีมาอย่างต่อเนื่อง นักวิจัยรายหนึ่งระบุว่า เขาได้พยายามโจมตี Bitcoin แต่ก็ไม่ประสบความสำเร็จ[3] นั่นแสดงให้เห็นว่า ความปลอดภัยของ Bitcoin เป็นสิ่งท้าทาย หากผู้ถือ Bitcoin ไม่ระมัดระวัง เช่น ลบ Bitcoin โดยไม่ได้ตั้งใจ จะทำให้ Bitcoin สูญหายได้ หากผู้ถือ Bitcoin ไม่เก็บกุญแจส่วนตัวไว้เป็นความลับ จะทำให้ผู้อื่นสามารถขโมย Bitcoin ไปได้ ดังเช่นที่เกิดขึ้นในรายการทีวีบลูมเบิร์ก เมื่อพิธีกรแสดงบัตรของขวัญเป็นเงิน Bitcoin จำนวน 20 ดอลลาร์ที่ได้รับมาผ่านหน้าจอโทรทัศน์ในระหว่างการออกรายการสดเป็นเวลาเพียง10 วินาทีเท่านั้น ผู้ชมทางบ้านฉวยโอกาสใช้โทรศัพท์มือถือสแกน QR code และขโมย Bitcoin นั้นไปได้[21]

การแลกเปลี่ยน Bitcoin สามารถถูกโจมตีได้ ดังเช่น ในปี ค.ศ. 2012 แฮคเกอร์ขโมยเงิน 24,000 BTC จากตลาดแลกเปลี่ยน Bitfloor[22] จากนั้นในปี ค.ศ. 2013 Mt.Gox ซึ่งเป็นตลาดแลกเปลี่ยน Bitcoin ที่ใหญ่ที่สุดก็ถูกโจมตีด้วย Distributed Denial-of-Service (DDoS)[23] Dust Transaction เป็นตัวอย่างหนึ่งของการโจมตีแบบ Denial of Service โดยผู้โจมตีจะส่ง Transaction ขนาดเล็กจำนวนมากเข้าไปในระบบ ทำให้เปลืองเนื้อที่ใน Block Chain[24]

ปัญหาด้านความปลอดภัยล่าสุดของ Bitcoin ส่งผลให้ค่าเงินผันผวนมาก เมื่อทาง Mt.Gox ประกาศหยุดให้ถอนเงิน เนื่องจากพบ Bug ในซอฟแวร์ Bitcoin ปัญหาหนึ่งที่นักพัฒนาออกแบบนั้นทราบมาตั้งแต่ปี ค.ศ. 2011 คือ Transaction-Malleability เนื่องมาจากโพรโทคอลที่ออกแบบทำให้ค่า Signature ครอบคลุมเพียงบางส่วนของข้อความที่โอนเงิน แต่ไม่ครอบคลุม Transaction ID ทำให้สามารถเปลี่ยนแปลง Transaction ID ได้ถึงแม้จะทำรายการไปแล้ว ผู้โจมตีจงใจเปลี่ยน Transaction ID หลังทำรายการ ทำให้รายการโอนที่ถูกบันทึกใน Block Chain มี Transaction ID ไม่ตรงกับที่โอนออกไป ซอฟต์แวร์ของเว็บรับแลกเงินจะเข้าใจว่าการโอนไม่สำเร็จ จึงพยายามโอนซ้ำอีกครั้ง ปัญหานี้ส่งผลให้ Mt.Gox ประกาศหยุดถอนเงินและประกาศล้มละลายวันที่ 28 กุมภาพันธ์ที่ผ่านมา[25]

สรุป

ปัจจุบัน Bitcoin เป็นที่สนใจของสังคมมากขึ้น เนื่องจากเป็นเงินสกุลที่อยู่ในรูปแบบดิจิตอล สามารถใช้แลกเปลี่ยนสินค้าและบริการได้อย่างสะดวกรวดเร็ว การทำธุรกรรมมีราคาถูก และไม่จำเป็นต้องมีบุคคลที่สามเข้ามาเกี่ยวข้อง ทำให้ปริมาณการใช้ Bitcoin ในการทำธุรกรรมต่าง ๆ มีแนวโน้มที่เพิ่มขึ้น อย่างไรก็ดี ปัญหาและความเสี่ยงจากการใช้ Bitcoin ก็ยังสามารถพบได้ ทั้งความเสี่ยงในด้านความปลอดภัย และความผันผวนอย่างมากของมูลค่า การนำ Bitcoin มาใช้แทนเงินจริงอย่างแพร่หลายในทางปฏิบัติยังทำได้ยาก เนื่องจาก Bitcoin ยังขาดคุณสมบัติของเงินที่ดี เช่น คุณสมบัติในการรักษามูลค่า[6] นอกจากนี้การขาดความยอมรับในด้านกฎหมายเป็นอีกปัจจัยสำคัญที่ผู้ที่สนใจควรพิจารณาอย่างรอบคอบก่อนการเข้ามาใช้เงินเสมือนอย่าง Bitcoin

เอกสารอ้างอิง

1. Blognone. (2012). Bitcoin เมื่อโลกเทคโนโลยีปลดแอกการเงินจากธนาคาร. ค้นเมื่อ กุมภาพันธ์ 24, 2557, จาก http://www.blognone.com/node/35180
2. Blognone. (2013). Bitcoin: การใช้งานและเหตุผลการออกแบบ. ค้นเมื่อ กุมภาพันธ์ 24, 2557, จาก http://www.blognone.com/node/47074

3. Brito, Jerry, and Andrea Castillo. “Bitcoin: A Primer for Policymakers.” *Mercatus Center: Geroge Mason University. http://mercatus. org/sites/default/files/ Brito_BitcoinPrimer_ embargoed. pdf* (2013).
4. Chaum, David. “Achieving electronic privacy.” (1992): 96-101.
5. Martin, Keith M. “Everyday Cryptography.” *The Australian Mathematical Society* (2012): 231.
6. Kasikornthai. “Bitcoin… เงินยุคดิจิตอล กับหลากความเสี่ยงที่ต้องคำนึงถึง.” กระแสทรรศน์: ปีที่ 20 ฉบับที่ 2470 (27 กุมภาพันธ์ 2557)
7. Nakamoto, Satoshi. “Bitcoin: A peer-to-peer electronic cash system.” *Consulted* 1 (2008): 2012.
8. WordPress.com. (2012). Pay Anouther Way: Bitcoin. ค้นเมื่อ กุมภาพันธ์ 24, 2557, จาก http://en.blog.wordpress.com/2012/11/15/pay-another-way-bitcoin/
9. Blognone. (2013). Namecheap รับ Bitcoin แล้ว. ค้นเมื่อ กุมภาพันธ์ 24, 2557, จาก http://www.blognone.com /node/41678
10. กรุงเทพธุรกิจ. (2556). เอทีเอ็มบิทคอยน์ตู้แรกของโลก. ค้นเมื่อ กุมภาพันธ์ 24, 2557, จาก http://www.bangkokbiznews.com/home/detail/finance/foreign/20131030/539844.html
11. TheNextWeb. (2014). Zynga is testing Bitcoin Payment for its Web games. ค้นเมื่อ กุมภาพันธ์ 24, 2557, จาก http://thenextweb.com/insider/ 2014/01/04/zynga-testing-bitcoin-payments-web-games
12. RTNEWS. (2013). Cash-for-bitcoins: World’s first palm scan-activated bitcoin ATM to open in Canada. ค้นเมื่อ กุมภาพันธ์ 24, 2557, จาก http://rt.com/news/bitcoin-atm-canada-first-799/
13. Blognone. (2014). Namecheap รับ Bitcoin แล้ว. ค้นเมื่อ มีนาคม 2, 2557, จาก http://www.blognone .com/node/53866
14. Snader, Robin, and Nikita Borisov. “A Tune-up for Tor: Improving Security and Performance in the Tor Network.” *NDSS*. Vol. 8. 2008.
15. Christin, Nicolas. “Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace.” *Proceedings of the 22nd international conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 2013.
16. REUTERS. (2013). FBI raids alleged online drug market Silk Road, arrests owner. ค้นเมื่อ มีนาคม 1, 2557, จาก http://www.reuters.com/ article/2013/10/02/crime-silkroad-raid-idUSL1N0HS12C20131002
17. Ron, Dorit, and Adi Shamir. “Quantitative analysis of the full bitcoin transaction graph.” *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2013. 6-24.
18. Blognone. (2013). พบความเชื่อมโยงระหว่างผู้สร้าง BitCoinและผู้ดูแล Silk Road. ค้นเมื่อ กุมภาพันธ์ 24, 2557, จาก http://www.blognone .com/node/51099
19. Blognone. (2013). ธุรกิจใหญ่ที่สุดใน BitCoin อาจจะเป็นการพนันออนไลน์. ค้นเมื่อ กุมภาพันธ์ 24, 2557, จาก http://www.blognone.com/node/ 47850
20. Blognone. (2014). เหตุผลใหม่ที่จะใช้ Bitcoin: ลูกค้า Porn.com จ่ายผ่าน Bitcoin 25%. ค้นเมื่อ กุมภาพันธ์ 24, 2557, จาก http://www.blognone .com/node/52585
21. ASTV. (2013). สุดมึน!! ผู้ชมทางบ้านขโมย “เงินบิทคอยน์” สกุลเงินโลกดิจิตอลใน “10 วินาที” หลังพิธีกร “ทีวีบลูมเบิร์ก” โชว์ออกอากาศสด. ค้นเมื่อ กุมภาพันธ์ 24, 2557, จาก http://www.manager .co.th/around/viewnews.aspx?NewsID=9560000158130
22. NBCNEWS. (2012). $250,000 worth of Bitcoins stolen in net heist. ค้นเมื่อ กุมภาพันธ์ 24, 2557, จาก http://www.nbcnews.com/ technology/250-000-worth-bitcoins-stolen-net-heist-980871
23. VB News. (2013). Fool me once: Bitcoin exchange Mt. Gox falls after third DDoS attack this month. ค้นเมื่อ กุมภาพันธ์ 24, 2557, จาก http://venturebeat.com/2013/04/21/mt-gox-ddos/
24. Bradbury, Danny. “The problem with Bitcoin.” *Computer Fraud & Security* 2013.11 (2013): 5-8.
25. Blognone. (2014). MtGox ถูกแฮกต่อเนื่องมาหลายปี เหลือ Bitcoin ในบัญชีเพียง 2,000 BTC. ค้นเมื่อ กุมภาพันธ์ 26, 2557, จาก http://www.blognone.com/node/53777
26. Miers, Ian, et al. “Zerocoin: Anonymous distributed e-cash from bitcoin.”*Security and Privacy (SP), 2013 IEEE Symposium on*. IEEE, 2013.
27. Singh, Prabhjot, et al. “Performance Comparison of Executing Fast Transactions in Bitcoin Network Using Verifiable Code Execution.” *Advanced Comput-*

ing, Networking and Security (ADCONS), 2013 2nd International Conference on. IEEE, 2013.

28. Herrmann, Matthias. *Implementation, evaluation and detection of a doublespend-attack on Bitcoin*. Diss. Master Thesis ETH Zürich, 2012, 2012.
29. Clark, Jeremy, and Aleksander Essex. "CommitCoin: carbon dating commitments with Bitcoin." *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2012. 390-398.
30. Huang, Danny Yuxing, et al. "Botcoin: monetizing stolen cycles." *Proceedings of NDSS*. Vol. 2014. 2014.
31. Skudnov,Rostislav."Bitcoinclients." *Instructor* 3.12 (2012): 32.
32. Sompolinsky, Yonatan, and Aviv Zohar. "Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains."
33. Reid, Fergal, and Martin Harrigan. "An analysis of anonymity in the bitcoin system." *Security and Privacy in Social Networks*. Springer New York, 2013. 197-223.
34. Bergstra, Jan A., and Karl de Leeuw. "Bitcoin and beyond: exclusively informational monies." *arXiv* (2013).
35. Decker, Christian, and Roger Wattenhofer. "Information propagation in the bitcoin network." *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*. IEEE, 2013.
36. Wallace, Benjamin. "The rise and fall of Bitcoin." *Wired Magazine. Available* (2011).
37. Karame, Ghassan, Elli Androulaki, and SrdjanCapkun. "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin." *IACR Cryptology ePrint Archive* 2012 (2012): 248.
38. Ober, Micha, Stefan Katzenbeisser, and Kay Hamacher. "Structure and anonymity of the bitcoin transaction graph." *Future Internet* 5.2 (2013): 237-250.
39. Babaioff, Moshe, et al. "On bitcoin and red balloons." *Proceedings of the 13th ACM Conference on Electronic Commerce*. ACM, 2012.
40 Bamert, Tobias, et al. "Have a snack, pay with Bitcoins." *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*. IEEE, 2013. Ateniese, Giuseppe, et al. "Certified Bitcoins."
41 Szefer, Jakub, and Ruby B. Lee. "BitDeposit: Deterring Attacks and Abuses of Cloud Computing Services Through Economic Measures." *Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium on*. IEEE, 2013.
42. Bedford Taylor, Michael. "Bitcoin and the age of Bespoke Silicon." *Compilers, Architecture and Synthesis for Embedded Systems (CASES), 2013 International Conference on*. IEEE, 2013.
43. Moore, Tyler, and Nicolas Christin. "Beware the middleman: Empirical analysis of Bitcoin-exchange risk." *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2013. 25-33.