นักสัญจรบนหน้ากระดาษ

ผู้แสวงหาความรู้และภูมิปัญญามาบรรณาการนักอ่าน

คริปโต
เงินแห่งโลกอนาคต จุดจบของธนาคาร
Cryptocurrency
How digital money could transform finance
จัน โวลปิเชลลี เขียน
วริษฐา กาลามเกษตร์ แปล
ราคา 325 บาท

First published as Cryptocurrency (WIRED guides): How Digital Money Could Transform Finance in 2021 by Cornerstone Digital, an imprint of Cornerstone. Cornerstone is part of the Penguin Random House group of companies.

ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ
National Library of Thailand Cataloging in Publication Data
โวลปิเชลลี, จัน.
คริปโต เงินแห่งอนาคต จุดจบธนาคาร = Cryptocurrency.-- กรุงเทพฯ : ยิปซี กรุ๊ป, 2569.
208 หน้า.
1. เงินดิจิทัล. 2. ธนาคารอิเล็กทรอนิกส์. I. วริษฐา กาลามเกษตร์, ผู้แปล. II. ชื่อเรื่อง.
332.178
ISBN 978-616-301-846-5

บรรณาธิการบริหาร	: คธาวุฒิ เกนุ้ย
บรรณาธิการอาวุโส	: สุรชัย พิงชัยภูมิ
บรรณาธิการเล่ม	: ทีฆทัศน์ มณีฉาย
หัวหน้ากองบรรณาธิการ	: ชยพฤกษ์ กองจันทร์
กองบรรณาธิการ	: คณิตา สุตราม พรรณิกา ครโสภา พิมพกานต์ เดชประสิทธิ์ศักดิ์
พิสูจน์อักษร	: กว่าชื่น บางคมบาง
รูปเล่ม	: บุษราภรณ์ สวนส่งผล
ออกแบบปก	: กิตติพล สรัคคานนท์
ผู้อำนวยการฝ่ายการตลาด	: นุชนันท์ ทักษิณาบัณฑิต
ผู้จัดการฝ่ายการตลาด	: ชิตพล จันสด
ผู้จัดการทั่วไป	: เวชพงษ์ รัตนมาลี
พิมพ์ที่	: บริษัท วิชั่น พรีเพรส จำกัด โทร. 0 2147 3175-6
จัดพิมพ์และจัดจำหน่ายโดย	: บริษัท ยิปซี กรุ๊ป จำกัด เลขที่ 37/145 รามคำแหง 98 แขวง/เขตสะพานสูง กรุงเทพฯ 10240 โทร. 0 2728 0939 โทรสาร 0 2728 0939 ต่อ 108 www.gypsygroup.net www.facebook.com/gypsygroup.co.ltd Line ID : @gypzy

คริปโต

เงินแห่งโลกอนาคต จุดจบของธนาคาร

CRYPTOCURRENCY

How digital money could transform finance

จัน โวลปิเชลลี เขียน

วริษฐา กาลามเกษตร์ แปล

คำนำสำนักพิมพ์

แม้ในปัจจุบันข่าวคริปโตเคอร์เรนซีมักปรากฏอยู่บนหน้าการเงินหรือเทคโนโลยี แต่จัน โวลปิเชลลี ผู้เขียนได้เน้นย้ำแต่แรกว่ามันเริ่มต้นจากการเมือง ดังนั้นเพื่อให้เราเข้าใจบทบาทของคริปโตเคอร์เรนซีต่อโลก เราอาจควรเข้าใจก่อนว่าจุดยืนทางการเมืองของมันอยู่ตรงไหน

เป้าหมายสำคัญของคริปโตเคอร์เรนซีตั้งแต่แรกเริ่ม (ในช่วงต้นทศวรรษที่ 1990) คือเพื่อสร้างสกุลเงินดิจิทัลที่เป็นอิสระจากการสอดส่องและควบคุมของรัฐโดยสิ้นเชิง รวมถึงปฏิเสธตัวกลางทางการเงิน เช่น ธนาคาร ซึ่งจะเข้ามามีอำนาจระหว่างการซื้อขายและการทำธุรกิจต่างๆ เพราะเหล่าผู้บุกเบิก (หรือที่เราจะรู้จักในนาม 'ไซเฟอร์พังก์') เชื่อว่าระบบการเงินในอุดมคตินั้นต้องปราศจากผู้เล่นที่มีอำนาจในการกำหนดทิศทาง และผู้ซื้อกับผู้ขายต้องสามารถเชื่อมโยงกันข้ามพรมแดนทุกประเทศทั่วโลกได้อย่างเสรี ดังนั้นเราจะเห็นว่าแนวคิดเรื่องการตัดตัวกลาง กระจายอำนาจ และลดทอนบทบาทของรัฐทั้งในภาคสังคมและเศรษฐกิจ รวมถึงแนวคิดเรื่องการค้าเสรีของมันสอดคล้องกับแนวคิดอิสรนิยมแบบขวา (right-libertarianism) [หากเรานึกภาพสเปกตรัมการเมือง ซึ่งเป็นเส้นแนวตั้ง (ภาคสังคม) และเส้นแนวนอน (ภาคเศรษฐกิจ) ตัดผ่านโดยตั้งฉากกัน แนวคิดอิสรนิยมจะอยู่

ฝั่งล่าง แนวคิดอำนาจนิยม (authoritarianism) จะอยู่ฝั่งบน ในขณะที่แนวคิดเศรษฐกิจฝั่งซ้ายจะเชื่อเรื่องการกระจายทรัพยากรอย่างเท่าเทียม ส่วนฝั่งขวาจะส่งเสริมการค้าเสรีภาคเอกชนและการลดบทบาทของรัฐ] เราจึงจะได้เห็นพลวัตของความเป็น 'ขวาล่าง' ของคริปโตเคอร์เรนซีในสังคมโลกตลอดกว่าสามทศวรรษที่ผ่านมาจากหนังสือเล่มนี้

ความน่าสนใจของหนังสือเล่มนี้อยู่ที่การนำเสนอประวัติศาสตร์ของคริปโตเคอร์เรนซีตั้งแต่ยุคพิมพ์เขียวมาจนถึงปัจจุบัน เพื่อเผยให้เห็นแนวคิดต่างๆ ที่ซ่อนอยู่ภายใต้ปรากฏการณ์นี้และผลกระทบของมันทั้งในด้านดีและร้าย รวมถึงชี้ให้เห็นว่าจากที่เคยเป็นเครื่องมือต่อต้านอำนาจรัฐสุดท้ายมันกลายเป็นเครื่องมือที่รัฐบาลของโดนัลด์ ทรัมป์ใช้ขณะดำรงตำแหน่งประธานาธิบดีของสหรัฐฯ สมัยแรกได้อย่างไร ดังนั้นไม่ว่าคุณจะเป็นสายคริปโต หรือไม่เคยสนใจเรื่องนี้มาก่อนเลย หนังสือเล่มนี้จะช่วยให้คุณเข้าใจที่มาที่ไปของคริปโตเคอร์เรนซีและความสำคัญของมันต่อโลกทั้งในแง่ของการเมือง เศรษฐกิจ และสังคมมากขึ้นอย่างแน่นอน

สำนักพิมพ์ยิปซี

คำนำผู้แปล

ไม่ว่าเรื่องราวของคริปโตเคอร์เรนซีดำเนินไปอย่างไร จะมีข่าวสาดโคลนหรือมีสาวกล้นหลาม จะเป็นภัยคุกคามหรือเป็นความหวังเรืองรอง ในฐานะผู้แปล บรรณาธิการหนังสือเกี่ยวกับคริปโตเคอร์เรนซีทั้งไทยและเทศ และนักอ่านทั่วไปคนหนึ่ง ยังเชื่อมั่นไม่ผันแปรว่าการทวนจุดกำเนิดและธรรมชาติของสิ่งที่เรียกว่าคริปโตเคอร์เรนซีซึ่งอยู่บนฐานนวัตกรรมที่ทรงพลังอย่างบล็อกเชนนั้นคุ้มค่าเสมอ ไม่ว่าคุณจะเป็นนักอ่านทั่วไปที่รักความรู้ เป็นนักลงทุน เซียนคริปโต หรือแค่สนใจเรื่องราวเชิงการเมือง ธุรกิจ และเศรษฐศาสตร์ เพราะไม่ว่าอย่างไรคริปโตเคอร์เรนซีคือหนึ่งในแลนมาร์กใหญ่คือจุดเริ่มต้นแห่งอนาคต ไม่ได้ต่างจากควอนตัมหรือเอไอที่มีผลต่อเรื่องราวการแตกเส้นทางของมนุษยชาติ ณ ตอนนี้และต่อจากนี้

พรสวรรค์การเป็นนักเล่าเรื่องและประสบการณ์ของจัน โวลปิเชลลี ผู้สื่อข่าวสายเทคโนโลยีของบลูมเบิร์กทำให้เล่มนี้เป็นคัมภีร์คริปโตที่แตกต่าง อ่านสนุก เข้มข้นแต่กระชับ ลึกแต่จับต้องได้และครอบคลุมอย่างไม่น่าเชื่อเท่าที่พื้นที่น้อยนิดแค่นี้จะทำได้ คุณยังได้คีย์เวิร์ดสำคัญทั้งหมดของโลกคริปโต ที่แค่ศัพท์แสงก็เปิดหูเปิดตาในตัวมันเอง นี่คือหนังสือที่เสริมมุมมองเชิงลึกทางการเมือง การเงิน และเศรษฐศาสตร์ ที่โยงใยอยู่กับนวัตกรรมเปลี่ยนโลกให้แก่คุณอย่างยอดเยี่ยม

ขอให้อ่านอย่างสนุก และขอขอบคุณสำนักพิมพ์ยิปซีที่วางใจให้ถ่ายถอดหนังสือเล่มเล็กที่ทรงพลังเล่มนี้ไว้ ณ ที่นี้ด้วยค่ะ

วริษฐา กาลามเกษตร์

27 เมษายน 2569

สารบัญ

บทนำ

คริปโตเคอร์เรนซี (cryptocurrency) คืออะไร คุณอาจตั้งคำถาม ซึ่งก็เหมือนคำถามทั่วๆ ไปที่เกี่ยวข้องกับคำจำกัดความที่มักมีหลายคำตอบนั่นแหละ คริปโตเคอร์เรนซีคือภาคธุรกิจที่กำลังเติบโตในวงการสตาร์ตอัปด้านเทคโนโลยี มันคือเงินดิจิทัลประเภทหนึ่ง คือ 'เหรียญ' (coin) อย่างบิตคอยน์ (Bitcoin) อีเธอร์ (Ether) หรือโมเนโร (Monero) นอกจากนี้ คริปโตเคอร์เรนซียังอาจเป็นช่องทางแสวงหาผลประโยชน์ในทางอาชญากรรมและการทุจริตได้เช่นกัน

โดยแก่นแท้ คริปโตเคอร์เรนซีคือเทคโนโลยีที่ใช้เทคนิคการเข้ารหัสลับ (cryptographic technique) ที่หลากหลายมาช่วยให้เราแลกเปลี่ยนหน่วยมูลค่า (unit of value) ระหว่างกันบนอินเทอร์เน็ตได้โดยไม่จำเป็นต้องพึ่งตัวกลางใดๆ เมื่อใช้คริปโตเคอร์เรนซี ตัวละครสมมติอย่างอลิซก็สามารถส่งหน่วยมูลค่าหนึ่งหน่วยไปให้ตัวละครสมมติอย่างบ็อบโดยไม่จำเป็น

ต้องมีธนาคาร บริษัทรับชำระเงิน หรือหน่วยงานรูปแบบใดๆ มาเกี่ยวข้อง ผู้รับรองความปลอดภัยของธุรกรรมนี้คือคอมพิวเตอร์ซึ่งทำงานร่วมกันแต่กระจายตัวอยู่ทั่วโลก และไม่มีเครื่องใดที่สามารถหยุดยั้งหรือแทรกแซงธุรกรรมดังกล่าวได้โดยพลการ

คริปโตเคอร์เรนซีได้เข้ามาท้าทายระบบการเงินที่ดำเนินมาหลายศตวรรษ ซึ่งหมายถึงระบบบนช่องทางที่มีตัวกลางและบุคคลที่สามเป็นผู้สร้างและดูแลรักษา ทั้งยังรับประกันว่าธุรกรรมต่างๆ ดำเนินไปอย่างซื่อสัตย์ นอกจากนี้คริปโตเคอร์เรนซียังเกิดขึ้นจากความพยายามที่จะอำนวยความสะดวกในการโอนเงินหรือตัวแทนของเงินโดยที่รัฐบาลไม่อาจรู้เห็นและควบคุมได้ เป้าหมายสูงสุดของมันคือ การตัดตัวกลาง (disintermediation) ซึ่งหมายถึงการตัดมนุษย์ออกจากขั้นตอนธุรกรรมและการสื่อสารต่างๆ ให้ได้มากที่สุด เหลือไว้เพียงปฏิสัมพันธ์โดยตรงระหว่างผู้ใช้กับผู้ใช้โดยไม่ต้องผ่านตัวกลาง (peer-to-peer หรือ P2P) (อย่างน้อยนี่ก็คือเจตนารมณ์ซึ่งในทางปฏิบัติยังไม่สมบูรณ์แบบในหลายกรณี)

คำตอบที่ว่านี้ค่อยๆ เบี่ยงออกจากโลกเทคโนโลยีมาสู่โลกปรัชญาการเมืองและข้อเท็จจริงที่ว่าคริปโตเคอร์เรนซีเป็นเรื่องการเมืองมากพอๆ กับเป็นเรื่องการเงิน เป้าหมายสำคัญอีกประการของมันคือการกระจายอำนาจ (decentralisation) หรือแนวคิดที่ว่าระบบไม่ควรมีผู้เล่นเพียงรายเดียว

หรือไม่กี่รายเป็นคนควบคุม ซึ่งการกระจายอำนาจและการตัดตัวกลางต่างเป็นเรื่องปกติในยุคอินเทอร์เน็ตเสียแล้ว เช่นเดียวกับบรรดานักการเมืองที่ก้าวข้ามสื่อหลักและผู้ตรวจสอบข้อมูลเพื่อไปเรียกเสียงโหวตทางทวิตเตอร์ หรือร้านค้าออนไลน์แบบหางยาว (เน้นขายสินค้าที่มีจำนวนน้อยให้ลูกค้าจำนวนมาก) แต่กลับสามารถเข้าถึงลูกค้าเฉพาะกลุ่มได้จนร้านค้าแบบเดิมๆ ต้องปิดตัวลงไปมากมาย ดังนั้นการที่คริปโตเคอร์เรนซีได้รับคำจำกัดความว่าเป็น 'เงินอินเทอร์เน็ต' (internet money) ในบางครั้งจึงฟังดูมีเหตุผลมากทีเดียว

หนังสือเล่มนี้จะช่วยอธิบายคำตอบอันหลากหลายเหล่านี้ให้กระจ่างขึ้น โดยพาคุณย้อนดูพัฒนาการของคริปโตเคอร์เรนซีในแต่ละขั้น ซึ่งจะเป็นตัวบอกเล่าประวัติศาสตร์ของมันตั้งแต่จุดกำเนิดเมื่อสามทศวรรษก่อนมาจนถึงพัฒนาการล่าสุด หนังสือเล่มนี้จึงเป็นดั่งบันทึกวิวัฒนาการของคริปโตเคอร์เรนซี รวมถึงหลักการที่ขับเคลื่อนมันไปข้างหน้าและแนวทางปฏิบัติของผู้ที่คิดค้นและสร้างมันขึ้นมา ตลอดทั้งห้าบท ซึ่งแต่ละบทจะเน้นไปที่คริปโตเคอร์เรนซีในแต่ละยุค (คำว่า 'ยุค' ในวงการนี้มีหน่วยเป็นหลักเดือนเท่านั้น) ผมจะพยายามตอบให้ละเอียดที่สุดเท่าที่จะทำได้ว่า 'คริปโตเคอร์เรนซีคืออะไร และทำไมเราควรสนใจมัน'

เตรียมตัวให้พร้อม การผจญภัยนี้น่าตื่นเต้นทีเดียว

1
บิตคอยน์ (Bitcoin)
จุดเริ่มต้นของคริปโต

ในตอนแรก คริปโตเคอร์เรนซีถือกำเนิดขึ้นในฐานะโปรเจกต์ทางการเมือง เราลืมเรื่องนี้ได้ง่ายๆ เพราะข่าวสารส่วนใหญ่เกี่ยวกับบิตคอยน์หรืออีเธอเรียมมักไปปรากฏในหน้าการเงิน สื่อด้านเทคโนโลยี หรือเว็บไซต์เฉพาะทางที่รายงานมูลค่าอันผันผวนของเหรียญดิจิทัลต่างๆ ได้อย่างละเอียด

ในแง่หนึ่ง เราอาจมองได้ว่าคริปโตเคอร์เรนซีคือผลลัพธ์ของการทดลองหลายทศวรรษเพื่อให้ได้มาซึ่งเทคโนโลยีที่ทำลายแนวคิดพื้นฐานของสิ่งที่เรียกว่ารัฐบาล เทคโนโลยีที่ว่าก็คือสกุลเงินดิจิทัลที่ไม่ขึ้นตรงกับรัฐ (stateless digital money) นั่นเอง

คนที่พยายามบรรลุเป้าหมายนี้เรียกตนเองว่า 'ไซเฟอร์พังก์' (cypherpunk)* ซึ่งประกอบด้วยนักเทคโนโลยี นักวิชาการ

* ล้อคำว่า 'ไซเบอร์พังก์' (cyberpunk) โดยใช้คำว่า 'cypher' ซึ่งแปลว่าการเข้ารหัสแทน ส่วน 'punk' แปลว่าพวกขบถสังคม – ผู้แปล

และนักคิดที่รวมกลุ่มกันอย่างไม่เป็นทางการ พวกเขานัดพบกันครั้งแรกแถวอ่าวซานฟรานซิสโกในช่วงต้นทศวรรษที่ 1990 และต่อมาได้ร่วมกันก่อตั้งกลุ่มสนทนาออนไลน์ทางอีเมลชื่อ 'Cypherpunks Mailing List' กลุ่มไซเฟอร์พังก์ถือกำเนิดขึ้นเมื่อคุณรวมเทคโนโลยีดิจิทัลเข้ากับแนวคิดอิสรนิยม (libertarianism)* ในมุมมองของกลุ่มไซเฟอร์พังก์ อินเทอร์เน็ตได้กลายเป็นพื้นที่แห่งอิสรภาพ สิทธิส่วนบุคคล การเชื่อมสัมพันธ์ และการแบ่งปันข้อมูลอย่างไร้ข้อจำกัด ซึ่งศัตรูของอุดมคตินี้คือรัฐบาลที่พยายามควบคุมอินเทอร์เน็ต ใช้มันเพื่อสอดแนมผู้ใช้งาน และสร้างอินเทอร์เน็ตขึ้นใหม่ให้เป็นเครื่องมือทำลายอิสรภาพจนทำให้เกิดการสอดส่องตรวจตราอยู่ทุกหนแห่งบนโลก จุดนี้เองทำให้วิทยาการเข้ารหัสลับ (cryptography) ที่แข็งแกร่งเข้ามามีบทบาท กลุ่มไซเฟอร์พังก์หวังว่าเครื่องมือต่างๆ เช่น อีเมลเข้ารหัส เครือข่ายนิรนาม และระบบการยืนยันตัวตนที่ปลอดภัยจะช่วยให้ผู้ใช้อินเทอร์เน็ตรอดพ้นจากการสอดแนมของรัฐบาลและพฤติกรรมใดๆ ก็ตามที่ส่อไปในทางการสอดส่องอย่างเข้มงวด ในระยะยาว เมื่อผู้คนส่วนใหญ่ใช้เทคโนโลยีเข้ารหัสกันได้แล้ว กฎหมายและข้อบังคับต่างๆ ในระดับชาติจะสูญเสียบทบาทในโลกไซเบอร์ลงเรื่อยๆ ข้อมูลจะหลั่งไหลถ่ายโอนได้อย่างเสรี ตลาดออนไลน์

* เน้นเสรีภาพของปัจเจกและเศรษฐกิจ มองว่ารัฐควรเข้ามาควบคุมให้น้อยที่สุด ต่างจากลัทธิเสรีนิยม (liberalism) ที่มุ่งเน้นสิทธิเสรีภาพเช่นกัน แต่มองว่ารัฐบาลควรมีบทบาทสำคัญในการบริหารจัดการสิ่งเหล่านี้

ที่ขายทุกอย่างตั้งแต่ไฟล์เพลงติดลิขสิทธิ์ไปจนถึงความลับของอุตสาหกรรมจะผุดพรายทั่วอินเทอร์เน็ต

ภาพอุดมคติดังกล่าวมีปลายทางอยู่ที่สภาวะอนาธิปัตย์คริปโต (crypto-anarchy) ซึ่งเป็นคำศัพท์ที่ทิโมธี เมย์ (Timothy May) นักวิทยาศาสตร์ของบริษัทอินเทลและไซเฟอร์พังก์คนสำคัญใช้ในบทความปี 1992 ซึ่งมีชื่อตรงไปตรงมาว่า 'The Crypto Anarchist Manifesto'[1] (แถลงการณ์นักอนาธิปไตยคริปโต) ตามที่เมย์อธิบายในบทความอีกชิ้นที่ยาวกว่านั้นในภายหลัง[2] สภาวะอนาธิปัตย์คริปโตหมายถึงการล่มสลายของรัฐบาลและการถือกำเนิดของระบอบการเมืองใหม่ที่ 'ปราศจากผู้ปกครองและกฎหมายภายนอก จะมีเพียงการปกครองรูปแบบเดียวเท่านั้น นั่นคือการจัดระเบียบโดยสมัครใจและได้รับการสนับสนุนจากสถาบันที่มีการจัดตั้งขึ้นโดยสมัครใจ […]' คำว่า 'คริปโต' ในคำว่า 'สภาวะอนาธิปัตย์คริปโต' นั้นเป็นทั้งคำเหน็บแนมทางการเมืองเหมือนคำว่า 'คริปโตฟาสซิสต์' (crypto-fascist) และเป็นการยอมรับอย่างจริงจังว่าเทคโนโลยีการเข้ารหัสลับจะเข้ามามีบทบาทสำคัญในการกระตุ้นให้เกิดการเปลี่ยนแปลงทางที่ดีเพื่อไปสู่ 'ระบบหนึ่งซึ่งจะพัฒนาขึ้นเมื่อโลกไซเบอร์มีความสำคัญยิ่งขึ้น ระบบที่อยู่ได้โดยปราศจากพรมแดนประเทศและตั้งอยู่บนฐานของการค้าเสรีโดยสมัครใจ (แม้จะนิรนามก็ตาม) สิ่งที่สำคัญที่สุดคือ รัฐบาลแบบที่เรารู้จักกันในวันนี้จะสิ้นสุดลง' ไม่มีพรมแดน ไม่มีภาษี ไม่มีกฎหมาย

ใช่ว่าไซเฟอร์พังก์ทุกคนจะต่อต้านรัฐบาลอย่างหนักหน่วงเหมือนเมย์ ซึ่งเป็นนักอุดมการณ์สุดโต่งผู้มีแนวคิดการเมืองที่อาจพัฒนาไปสู่อุดมการณ์แบบขวาจัดในที่สุด* แต่อย่างน้อยที่สุด สมาชิกส่วนใหญ่ของกลุ่ม Cypherpunks Mailing List ที่มีกันกว่า 700 คน รวมถึง อดัม แบ็ก (Adam Back) นักธุรกิจชาวอังกฤษ ริชาร์ด สตอลล์แมน (Richard Stallman) นักทฤษฎีซอฟต์แวร์เสรี และจูเลียน อัสซานจ์ (Julian Assange)[3] ผู้ที่จะก่อตั้งเว็บไซต์ 'วิกิลีกส์' (WikiLeaks) ในอนาคต ต่างมองว่าความเป็นส่วนตัวเป็นสิ่งพึงปรารถนาและการสอดส่องเป็นสิ่งอันตราย ทั้งยังเฝ้าฝันถึงโลกอินเทอร์เน็ตที่ปราศจากการควบคุมของรัฐบาล

เมื่อกลุ่มไซเฟอร์พังก์เริ่มร่างวิสัยทัศน์ของตนออกมาชิ้นส่วนบางอย่างก็เริ่มเข้าที่เข้าทาง มีการเปิดตัวพีจีพี (PGP - Pretty Good Privacy) โปรแกรมเข้ารหัสการสื่อสารออนไลน์ในปี 1991 ขณะเดียวกัน โปรแกรมส่งต่ออีเมลแบบนิรนาม (anonymous remailers) ที่ช่วยให้เราส่งต่ออีเมลไปยังผู้รับที่ต้องการโดยไม่ต้องระบุตัวผู้ส่งก็ได้รับความนิยมมากขึ้นเรื่อยๆ ทำให้การปกปิดตัวตนแน่นหนาขึ้นอีกชั้น เหลืออีกสิ่งหนึ่งที่ยังจับต้องยาก นั่นคือเงินดิจิทัลแบบนิรนาม (anonymous digital cash)

---

* แนวคิดการเมืองแบบเสรีนิยมสุดโต่ง – ผู้แปล

เป้าหมายแบบอิสรนิยมสูงสุดของกลุ่มไซเฟอร์พังก์ไม่อาจละทิ้งแก่นของแนวคิดอิสรนิยมได้ นั่นคือตลาดเสรี (free market) เมย์มองว่าโลกไซเบอร์ไม่เพียงแต่จะกลายเป็นชุมชนของการสื่อสารนิรนามที่ไร้สิ่งกีดขวางเท่านั้น แต่ยังเป็นตลาดขนาดใหญ่สำหรับซื้อขายและแลกเปลี่ยนสินค้า บริการ และข้อมูล ทั้งแบบถูกกฎหมายและผิดกฎหมาย[4] ทำให้เกิดปัญหาว่าธุรกรรมเหล่านั้นควรใช้สกุลเงินอะไร แน่นอนว่าระบบชำระเงินอิเล็กทรอนิกส์ (electronic payment systems) ที่เป็นบริการของธนาคารหรือบริษัทบัตรเครดิตย่อมไม่ใช่ทางเลือก เพราะในระบบนี้ผู้ชำระเงินและผู้รับชำระต้องใช้ชื่อจริง ซึ่งขัดกับหลักความเป็นนิรนามที่กลุ่มไซเฟอร์พังก์เชิดชูบูชา ที่ร้ายแรงกว่านั้นคือระบบดังกล่าวได้ทิ้งข้อมูลที่รัฐบาลสามารถเรียกตรวจสอบเพื่อวัตถุประสงค์ของการกำกับดูแลหรือเพื่อดำเนินคดีในกรณีที่มีการค้าผิดกฎหมายได้ ในฐานะไซเฟอร์พังก์รุ่นบุกเบิกอีกคนหนึ่ง เอริค ฮิวส์ (Eric Hughes) ได้เขียนบทความชื่อ 'A Cypherpunk Manifesto' (แถลงการณ์ของไซเฟอร์พังก์) ซึ่งตีพิมพ์ทางออนไลน์ในปี 1993 โดยมีข้อความว่า 'ความเป็นส่วนตัวในสังคมแบบเปิดจำเป็นต้องมีระบบธุรกรรมแบบนิรนาม'[5] ซึ่งฮิวส์เสริมว่าปกติแล้วจะเกิดขึ้นได้ต่อเมื่อเราใช้เงินสด

แต่เงินสดก็ถูกมองว่าแย่เช่นกันด้วยเหตุผลหลายประการ เช่น เหตุผลในเชิงกายภาพ คงไม่เข้าท่าหากเราจะขับเคลื่อนตลาดออนไลน์แบบนิรนามโดยการส่งธนบัตรเป็น

ฟ่อนให้กันทางไปรษณีย์ หรือที่แย่กว่านั้นคือยื่นให้กันตัวต่อตัวซึ่งดูเสี่ยง นอกจากนี้ยังมีเหตุผลเชิงแนวคิดอื่นๆ เช่น แม้ไซเฟอร์พังก์จะไม่ได้อยากให้รัฐบาลหายไปโดยสิ้นเชิงทุกคน แต่หลายคนก็เชื่อในหลักเศรษฐศาสตร์ออสเตรีย (Austrian School of economics)[6] ซึ่งพัฒนาขึ้นในกรุงเวียนนาช่วงปลายศตวรรษที่ 19 และต้นศตวรรษที่ 20 โดยมีนักคิดคนสำคัญได้แก่ ฟรีดริช ฟอน ฮาเย็ก (Friedrich von Hayek) บุคคลที่มาร์กาเรต แธตเชอร์ (Margaret Thatcher) ชื่นชอบ ผู้สนับสนุนสำนักคิดนี้ไม่เห็นด้วยกับการใช้สกุลเงินที่ออกโดยรัฐบาล เพราะเชื่อว่าเงินควรมีมูลค่าและเสถียรภาพในตัวเองเหมือนทองคำและเงิน (ที่เป็นธาตุ) เมื่อสกุลเงินของรัฐบาลไม่เป็นเช่นนั้น (เช่นเดียวกับสกุลเงินต่างๆ ในปัจจุบันที่รัฐบาลเป็นผู้กำหนดมูลค่ามากกว่าการที่มันจะสามารถนำมาแลกเปลี่ยนเป็นโลหะมีค่าได้ด้วยตัวของมันเอง) บรรดานักเศรษฐศาสตร์ชาวออสเตรียจึงกลัวว่าธนาคารกลางจะใช้นโยบายเพิ่มหรือลดมูลค่าสกุลเงินตามอำเภอใจ ซึ่งจะสร้างความเสียหายต่อผู้ให้กู้ในภาวะเงินเฟ้อและต่อผู้กู้ในภาวะเงินฝืด ทางออกหนึ่งที่ฮาเย็กเสนอในหนังสือ *The Denationalisation of Money (การคืนอำนาจทางการเงินให้แก่ประชาชน)*[7] ที่เขาเขียนคือการให้ประชาชนและบรรดาองค์กรเอกชนออกสกุลเงินมาแข่งขันกัน รวมถึงแข่งกับสกุลเงินที่ถูกกฎหมายจากรัฐบาลด้วย แล้วให้ผู้ใช้ตัดสินใจเองว่าจะใช้เงินสกุลใดในการซื้อขาย ฮาเย็กมองว่าวิธีนี้จะทำให้ตลาดเต็มไปด้วยสกุลเงินที่

แข็งแกร่งที่สุด โดยรัฐบาลไม่อาจทำลายมูลค่าของมันได้ตามอำเภอใจด้วยนโนบายที่ก่อให้เกิดภาวะเงินเฟ้อได้เลย

กลุ่มไซเฟอร์พังก์จึงต้องการสิ่งอื่นที่ไม่ใช่เงินสดหรือสกุลเงินอิเล็กทรอนิกส์ใดๆ ที่ออกโดยธนาคาร เป็นสิ่งใหม่ที่มีความเป็นนิรนามเหมือนธนบัตร แต่รวดเร็วและครอบคลุมทั่วโลกเหมือนการโอนเงินอิเล็กทรอนิกส์ และหากเป็นไปได้ ต้องมีเสถียรภาพอย่างที่บรรดานักเศรษฐศาสตร์ชาวออสเตรียต้องการด้วย ซึ่งนั่นไม่ใช่เรื่องง่าย

ปัญหาแรกในการผลิตสกุลเงินเช่นนั้นคือการจ่ายซ้ำซ้อน (double-spending) เมื่อคุณพยายามสร้างสกุลเงินดิจิทัลขึ้นมาหนึ่งหน่วย คุณมีโอกาสที่จะได้สิ่งที่เหมือนไฟล์หนึ่งไฟล์ซึ่งน่าจะมาพร้อมกับตัวอักษรชุดหนึ่งที่ทำให้มันมีความเฉพาะตัวเหมือนเลขธนบัตร แต่ธนบัตรเป็นวัตถุที่ประกอบขึ้นจากอะตอม ในขณะที่ธนบัตรดิจิทัลที่เราสมมติอยู่นี้ประกอบขึ้นจากหน่วยข้อมูลที่เรียกว่าบิต (bits) และนั่นคือปัญหา เมื่อมีการใช้ธนบัตรกระดาษ ธนบัตรใบนั้นจะถูกเปลี่ยนมือ หมายความว่าคุณจะมีธนบัตร 10 ดอลลาร์สหรัฐอยู่กับตัวหรือไม่ก็ไม่มี มีแค่สองทางเลือกเท่านั้น แต่หากเป็นไฟล์ เราสามารถส่งให้ผู้รับหลายคนได้ในหลายๆ ครั้ง ผู้ใช้เงินดิจิทัลที่ไม่ซื่อสัตย์อาจตัดสินใจใช้สกุลเงินหน่วยเดิมซ้ำๆ หรือที่เรียกว่าการจ่ายซ้ำซ้อน ถือเป็นภัยคุกคามสำคัญที่ส่งผลต่อความพยายามจะสร้างระบบชำระเงินที่มีประสิทธิภาพ ทางแก้ที่ตรงไปตรงมาที่สุดก็คือ ให้มีผู้ตัดสินใจซึ่งเป็นบุคคลที่สาม