

O'REILLY®



Mastering the Lightning Network

พลิกโลกการชำระเงิน บนบิตคอยน์บล็อกเชน

ไลต์นิงเน็ตเวิร์ก : โพรโทคอลชั้นที่สองบน
บิตคอยน์บล็อกเชนสำหรับการชำระเงินแบบทันที

อธิบายการทำงาน เทคนิค และวิธีการอย่างละเอียด



เขียน

Andreas M. Antonopoulos,
Olaoluwa Osuntokun
& René Pickhardt

แปล

พศ. ดร.ธนฤกษ์ รณกิจสมบัติ



มีเพียง “ความรู้” เท่านั้นที่มนุษย์ใช้พลิก “โลก”
และเปลี่ยน “ชีวิต” เราจึงสร้างสรรค์ และส่งมอบ “ความรู้”
ในรูปแบบที่ดีกว่า เพื่อให้คนไทย “เรียนรู้” ได้ตลอดชีวิต

Only “Knowledge” can help human
change “The World” and “Their Lives”.
With this truth, it drives us to deliver
“Knowledge” for Thai being able to
“Learn” better everyday.



Think
Beyond



Mastering the Lightning Network

พลิกโลกการชำระเงินบนบิตคอยน์บล็อกเชน

Writers	แอนเดรียส เอ็ม. แอนโทโนปูลอส (Andreas M. Antonopoulos), โอลาลูว่า โอซุนโทกุน (Olaoluwa Osuntokun), เรเน่ พิคการ์ดท์ (René Pickhardt)
Translator	ผศ. ดร.ธนฤกษ์ ธนกิจสมบัติ
Academic Editor	ภิรพล คชาเจริญ
Executive Editors	สัจจะ จรัสรุ่งรวิธร, อรรณพ ชันธิกุล
Production Manager	วรพล ณิชกุล
Graphic Designer	ชวรินทร์ รัตนะ
Page Layout	สุวิสวัสดิ์ วงศ์จันทร์สุข
Proofreader	พรณรัตน์ ขุราณี
Publishing Coordinators	สุรีย์รัตน์ จิ๋ว, นัตรตนัย ศรีสวัสดิ์
Product Specialist	ระพีพัฒน์ โทจำปา

© 2024 IDC Premier Company Limited

Authorized Thai translation of the English edition of Mastering the Lightning Network
ISBN 9781492054863 © 2022 aantonop Books LLC, René Pickhardt, and uuddlrlrbas LLC.

This translation is published and sold by permission of O'Reilly Media, Inc., which owns or controls all rights to publish and sell the same. Thai translation arranged through Little Rainbow Agency.

สงวนลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 โดยบริษัท ไอดีซี พรีเมียร์ จำกัด ห้ามลอกเลียนไม่ว่าส่วนใดส่วนหนึ่งของหนังสือเล่มนี้ ไม่ว่าในรูปแบบใดๆ นอกจากจะได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้จัดพิมพ์เท่านั้น

สร้างสรรคโดย



ข้อมูลทางบรรณานุกรม

แอนเดรียส เอ็ม. แอนโทโนปูลอส (Andreas M. Antonopoulos)
Mastering the Lightning Network
พลิกโลกการชำระเงินบนบิตคอยน์บล็อกเชน
นนทบุรี : ไอดีซี, 2567
488 หน้า

1. โปรแกรมสำหรับการ

ประมวลผลข้อมูลเฉพาะชนิด

I โอลาลูว่า โอซุนโทกุน (Olaoluwa Osuntokun)

II เรเน่ พิคการ์ดท์ (René Pickhardt) ผู้แต่งร่วม

III ชื่อเรื่อง

005.37

ISBN 978-616-487-530-2

พิมพ์ครั้งที่ 1 พฤษภาคม 2567

ราคา 750 บาท

จัดพิมพ์และจัดจำหน่ายโดย



บริษัท ไอดีซี พรีเมียร์ จำกัด

200 หมู่ 4 ชั้น 19 ห้อง 1901

อาคารจัสตินอินเตอร์เนชั่นแนลทาวเวอร์

ถ.แจ้งวัฒนะ อ.ปากเกร็ด จ.นนทบุรี 11120

โทรศัพท์ 0-2962-1081 (อัตโนมัติ 10 คู่สาย)

โทรสาร 0-2962-1084

สมาชิกสัมพันธ์

โทรศัพท์ 0-2962-1081-3 ต่อ 121

โทรสาร 0-2962-1084

ร้านค้าและตัวแทนจำหน่าย

โทรศัพท์ 0-2962-1081-3 ต่อ 112-114

โทรสาร 0-2962-1084

พิมพ์ที่ บริษัท ดี.เค.ปรี้นติ้ง จำกัด

441/56 หมู่ 2 ต.บางบ่อ อ.บางบ่อ

จ.สมุทรปราการ 10560

โทรศัพท์ 0-2115-9105 โทรสาร 0-2115-9044

คำนำผู้เขียน

ไลต์นิงเน็ตเวิร์ก เป็นเครือข่ายแบบไร้ตัวกลางในเลเยอร์ที่สอง ที่ช่วยให้เราสามารถทำการชำระเงินบิตคอยน์แบบ “Off-chain” ได้ โดยไม่ต้องทำการสร้างธุรกรรมบนบิตคอยน์บล็อกเชน

ไลต์นิงเน็ตเวิร์กทำให้การชำระเงินบิตคอยน์มีความปลอดภัย ราคาถูก รวดเร็ว และมีความเป็นส่วนตัวขึ้นมาก แม้จะเป็นเพียงการชำระเงินในปริมาณเล็กน้อยก็ตาม

ไลต์นิงเน็ตเวิร์กแท้จริงแล้วคือเครือข่ายของแชนเนลการชำระเงิน ที่ซึ่งการชำระเงินจะเดินทางไปตามเส้นทางที่เชื่อมต่อแชนเนลการชำระเงินต่างๆ จากผู้ส่งไปยังผู้รับ อันเป็นการต่อยอดมาจากแนวความคิดในเรื่องของแชนเนลการชำระเงินที่ถูกนำเสนอเป็นครั้งแรกโดย Satoshi Nakamoto ผู้ให้กำเนิดบิตคอยน์

แนวคิดเกี่ยวกับ “ไลต์นิงเน็ตเวิร์ก” ได้ถูกนำเสนอขึ้นเป็นครั้งแรกในปี 2015 ในบทความล้ำสมัยที่ชื่อว่า “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments” ซึ่งถูกเขียนขึ้นโดย Joseph Poon และ Thaddeus Dryja และในปี 2017 ก็ได้มีไลต์นิงเน็ตเวิร์กเวอร์ชัน “ทดสอบ” รันอยู่บนอินเทอร์เน็ต อันเกิดจากการที่กลุ่มต่างๆ ได้สร้างระบบการใช้งานที่แตกต่างกันแต่สามารถเทียบเคียงกันได้ และได้ประสานงานเพื่อกำหนดมาตรฐานการทำงานร่วมกัน และในที่สุดไลต์นิงเน็ตเวิร์กเวอร์ชัน “จริง” ก็ได้ถือกำเนิดขึ้น และเริ่มมีการชำระเงินผ่านไลต์นิงเน็ตเวิร์กเป็นครั้งแรกในปี 2018

ในปี 2019 Andreas M. Antonopoulos, Olaoluwa Osuntokun และ René Pickhardt ตกลงที่จะร่วมมือกันเขียนหนังสือเล่มนี้ขึ้นมา และดูเหมือนเราจะทำสำเร็จแล้ว!

หนังสือเล่มนี้เหมาะสำหรับผู้อ่านที่มีความรู้ด้านเทคนิค และมีความเข้าใจในหลักการพื้นฐานของระบบบิตคอยน์และบล็อกเชนแบบเปิดอื่นๆ

Andreas M. Antonopoulos,
Olaoluwa Osuntokun
และ René Pickhardt



คำนำผู้แปล

ในยุคที่เทคโนโลยีบล็อกเชนกำลังพัฒนาไปอย่างรวดเร็ว “Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments” เป็นหนังสือที่ไม่ควรพลาดอย่างยิ่งสำหรับผู้ที่ต้องการศึกษาเกี่ยวกับไลต์นิงเน็ตเวิร์ก (Lightning Network) – นวัตกรรมสำคัญที่จะทำให้การชำระเงินบิตคอยน์สามารถทำได้อย่างรวดเร็วขึ้น มีความเป็นส่วนตัวมากขึ้น และมีราคาถูกลง

การแปลหนังสือเล่มนี้เป็นภาษาไทยถือเป็นงานที่ท้าทาย และเต็มไปด้วยความภาคภูมิใจ ซึ่งผมได้พยายามอย่างยิ่งในการรักษาความหมายและเสน่ห์ของต้นฉบับไว้ ทั้งยังปรับให้เข้ากับบริบททางเทคนิค เพื่อให้ผู้อ่านชาวไทยสามารถเข้าถึงและเข้าใจได้ง่ายขึ้น

แม้ว่าจะมีเนื้อหาทางเทคนิคค่อนข้างมาก และเหมาะกับผู้ที่มีความรู้พื้นฐานเกี่ยวกับบิตคอยน์และบล็อกเชนอยู่แล้ว แต่หนังสือเล่มนี้ก็ถูกเขียนขึ้นด้วยสไตล์ที่อ่านง่ายและเข้าใจได้ไม่ยากนัก ผู้ที่มีความสนใจอย่างแรงกล้าในการทำความเข้าใจ แต่ยังไม่มีความรู้เบื้องต้น ก็สามารถใช้นี้หนังสือเล่มนี้เป็นคู่มือเริ่มต้นเรียนรู้เทคโนโลยีที่มีศักยภาพในการเปลี่ยนแปลงโลกอย่างไลต์นิงเน็ตเวิร์กได้เช่นกัน

ในฐานะผู้แปล ผมหวังว่าการแปลงานเขียนเล่มนี้เป็นภาษาไทย จะทำให้ผู้อ่านชาวไทยสามารถเข้าถึง และใช้ประโยชน์จากความรู้ที่มีคุณค่านี้ได้มากยิ่งขึ้น และที่สำคัญที่สุดคือ เพื่อให้ทุกคนสามารถมีส่วนร่วมในการสร้างอนาคตของการเงิน และเทคโนโลยีแบบไร้ตัวกลางนี้ไปด้วยกัน

ผศ. ดร.ธนฤทธิ์ ธนกิจสมบัติ

ภาควิชาบริหารธุรกิจ

วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล

thanarerk@gmail.com

CONTENTS

PART I ทำความเข้าใจกับไต่ตึงเน็ตเวิร์ก	18
CHAPTER 01 บทนำ	19
หลักการพื้นฐานของไต่ตึงเน็ตเวิร์ก	20
ความเชื่อถือว่าไว้วางใจในเครือข่ายแบบกระจายศูนย์ (Decentralized Networks)	22
ความยุติธรรมแบบไร้อำนาจส่วนกลาง (Central Authority)	22
โพรโทคอลในการสร้างความเชื่อถือว่าไว้วางใจแบบไร้ตัวกลาง	23
การทำงานของโพรโทคอลสร้างความยุติธรรม	25
ความมั่นคงปลอดภัยพื้นฐานเป็นส่วนประกอบที่สำคัญ	26
ตัวอย่างของโพรโทคอลสร้างความยุติธรรม	27
แรงจูงใจของการมีไต่ตึงเน็ตเวิร์ก	28
การขยายบล็อกเชน (Scaling Blockchains)	29
คุณลักษณะของไต่ตึงเน็ตเวิร์ก	31
กรณีศึกษาการใช้งานไต่ตึงเน็ตเวิร์ก	32
สรุปประจำบท	33
CHAPTER 02 มาเริ่มต้นกัน	35
กระเป๋าเงินไต่ตึงแรกของแอลิช	35
ไต่ตึงโหนด (Lightning Nodes)	36
Lightning Explorers	36
กระเป๋าเงินไต่ตึง (Lightning Wallets)	37
Testnet Bitcoin	41
สมดุลระหว่างความซับซ้อนกับการควบคุม	42
การดาวน์โหลดและติดตั้งกระเป๋าเงินไต่ตึง (Lightning Wallet)	43
การสร้างกระเป๋าเงินใหม่ (New Wallet)	44
ความรับผิดชอบในการเก็บรักษากุญแจเข้ารหัส (Key Custody)	44
คำช่วยจำ (Mnemonic Words)	44
การเก็บรักษาคำช่วยจำอย่างปลอดภัย (Storing the Mnemonic Safely)	45
การเติมเงินบิตคอยน์เข้ากระเป๋าเงิน	46
การได้มาซึ่งเงินบิตคอยน์	46
การรับเงินบิตคอยน์	47
จาก Bitcoin สู่ Lightning Network	50
แบบแผนไต่ตึงเน็ตเวิร์ก (Lightning Network Channels)	51
การเปิดไต่ตึงแบบแนว (Lightning Channel)	53

การซื้อกาแฟแก้วหนึ่งโดยใช้ไลต์นิงเน็ตเวิร์ก	55
Bob's Cafe	56
Lightning Invoice	57
สรุปประจำบท	59
CHAPTER 03 ไลต์นิงเน็ตเวิร์กทำงานอย่างไร	61
แชนเนลชำระเงิน (Payment Channels) คืออะไร	62
ความรู้พื้นฐานเกี่ยวกับแชนเนลชำระเงิน	63
การใช้เส้นทางชำระเงิน (Routing Payments) ผ่านแชนเนล	64
แชนเนลชำระเงิน (Payment Channels)	65
ที่อยู่บิตคอยน์แบบหลายลายเซ็น (Multisignature Address)	66
ธุรกรรมการฝากเงิน (Funding Transaction)	66
ธุรกรรมพันธสัญญา (Commitment Transaction)	68
การทุจริตโดยใช้สถานะก่อนหน้า (Cheating with Prior State)	70
การประกาศแชนเนล (Announcing the Channel)	73
การปิดแชนเนล (Closing the Channel)	74
ใบแจ้งหนี้ (Invoice)	80
Payment Hash และ Preimage	81
ข้อมูลลอททิฟเพิ่มเติม (Metadata)	81
การส่งการชำระเงิน	82
โพรโทคอลแบบซุบซิบแบบไร้ตัวกลาง (The Peer-to-Peer Gossip Protocol)	82
การค้นหาและการใช้เส้นทาง (Pathfinding and Routing)	84
การค้นหาเส้นทางแบบ Source-based	85
การใช้เส้นทางแบบ Onion Routing	86
อัลกอริทึมการส่งต่อการชำระเงิน (Payment Forwarding Algorithm)	88
การเข้ารหัสข้อมูลการสื่อสารแบบไร้ตัวกลาง (Peer-to-Peer)	89
มุมมองเกี่ยวกับความเชื่อถือได้ (Trust)	90
ข้อเปรียบเทียบกับระบบบิตคอยน์ (Comparison with Bitcoin)	90
ที่อยู่ เทียบกับ ใบแจ้งหนี้ (Address VS Invoice), ธุรกรรม เทียบกับ การชำระเงิน (Transaction VS Payment)	91
การเลือกเอาต์พุต เทียบกับ การค้นหาเส้นทาง (Selecting Outputs VS Finding a Path)	91
การเปลี่ยนแปลงเอาต์พุตบนระบบบิตคอยน์ เทียบกับ การไม่เปลี่ยนแปลงเอาต์พุตบนระบบไลต์นิง	
(Change Outputs on Bitcoin VS No Change on Lightning)	92
ค่าธรรมเนียมการขุด เทียบกับ ค่าธรรมเนียมการใช้เส้นทาง (Mining Fees VS Routing Fees)	92
ค่าธรรมเนียมที่ขึ้นอยู่กับจำนวนธุรกรรม เทียบกับ ค่าธรรมเนียมที่ถูกประกาศ	
(Varying Fees Depending on Traffic VS Announced Fees)	93
ธุรกรรมบิตคอยน์แบบสาธารณะ เทียบกับ การชำระเงินไลต์นิงที่เป็นส่วนตัว	
(Public Bitcoin Transactions VS Private Lightning Payments)	94

การรอการยืนยัน เทียบกับ การชำระบัญชีแบบเสร็จทันที (Waiting for Confirmations VS Instant Settlement)	94
การส่งเงินโดยกำหนดจำนวนเอง เทียบกับ การจำกัดความจุในการส่ง (Sending Arbitrary Amounts VS Capacity Restrictions)	95
แรงจูงใจในการชำระเงินจำนวนมาก เทียบกับ การชำระเงินจำนวนน้อย (Incentives for Large Value Payment VS Small Value Payments)	95
การใช้บล็อกเชนเป็นบัญชีบันทึกรูขุม เทียบกับ การเป็นระบบศาล (Blockchain as a Ledger VS as a Court System)	96
ออฟไลน์ เทียบกับ ออนไลน์ และ Asynchronous เทียบกับ Synchronous	96
Satoshis เทียบกับ Millisatoshis	97
ความเหมือนกันของระบบบิตคอยน์และระบบไลต์นิง	97
หน่วยเงิน (Monetary Unit)	97
การเปลี่ยนแปลงย้อนกลับไม่ได้ และการเสร็จสิ้นสมบูรณ์ของการชำระเงิน (Irreversibility and Finality of Payments)	97
ความเชื่อใจไว้ใจและความเสี่ยงจากคู่สัญญา (Trust and Counterparty Risk)	98
การดำเนินการโดยไม่ต้องได้รับอนุญาต (Permissionless Operation)	98
โอเพนซอร์สและระบบเปิด (Open Source and Open System)	98
สรุปประจำวัน	98
CHAPTER 04 ซอฟต์แวร์ไลต์นิงโนด	99
สภาพแวดล้อมสำหรับการพัฒนาระบบไลต์นิง (Lightning Development Environment)	100
การใช้บรรทัดคำสั่ง (Command Line)	100
การดาวน์โหลดคลังข้อมูลหนังสือ (Book Repository)	101
Docker Containers	102
Bitcoin Core และ Regtest	104
การสร้าง Bitcoin Core Container	104
โครงการ c-lightning ไลต์นิงโนด	107
การสร้าง c-lightning เป็น Docker Container	107
การติดตั้ง Docker Network	109
การรับ bitcoind และ c-lightning container	109
การติดตั้ง c-lightning จากซอร์สโค้ด	111
การติดตั้งคลังซอฟต์แวร์ (Libraries) และแพ็คเกจ (Packages) ที่จำเป็นต้องมีในเบื้องต้น	111
การคัดลอก c-lightning ซอร์สโค้ด	112
การแปล c-lightning ซอร์สโค้ด	112
โครงการ Lightning Network Daemon(LND) Node	114
LND Docker Container	115
การรับ bitcoind และ LND Container	116
การติดตั้ง LND จากซอร์สโค้ด	118
การคัดลอก LND ซอร์สโค้ด	119
การแปล LND ซอร์สโค้ด	119

โครงการ Eclair Lightning Node	120
Eclair Docker Container	120
การรับ bitcoind และ Eclair Containers	121
การติดตั้ง Eclair จากซอร์สโค้ด	123
การคัดลอก Eclair ซอร์สโค้ด	124
การแปล Eclair ซอร์สโค้ด	124
การสร้างเน็ตเวิร์กที่ประกอบไปด้วยโหนดหลายๆ ประเภท	125
การใช้ docker-compose ในการจัดการ Docker Containers	125
การตั้งค่าเริ่มต้น docker-compose	126
การเริ่มต้น Lightning Network สาธิต	127
การเปิดแชแนลและการใช้เส้นทางการชำระเงิน	128
สรุปประจำบท	130
CHAPTER 05 การรันโหนดบนไลต์นิงเน็ตเวิร์ก	131
การเลือกแพลตฟอร์ม	132
ความสำคัญของความน่าเชื่อถือในการรัน Lightning Node	132
ชนิดของฮาร์ดแวร์ Lightning Node	133
การรันบนคลาวด์ (Cloud)	133
การรันโหนดที่บ้าน	134
ฮาร์ดแวร์ที่จำเป็นในการรัน Lightning Node	135
การสลับการตั้งค่าเซิร์ฟเวอร์ในคลาวด์	136
การใช้ Installer หรือ Helper	137
RaspiBlitz	138
Mynode	139
Umbrel	139
BTCPay Server	141
Bitcoin Node หรือ Lightning แบบ Lightweight	142
ตัวเลือกของระบบปฏิบัติการ (Operating System)	143
การเลือกวิธีการใช้งาน Lightning Node	143
การติดตั้ง Bitcoin Node และ Lightning Node	144
บริการส่วนที่อยู่เบื้องหลัง (Background Services)	145
การแยกกระบวนการ (Process Isolation)	145
การเริ่มต้นโหนด (Node Startup)	146
การตั้งค่าเริ่มต้นของโหนด (Node Configuration)	147
การตั้งค่าเริ่มต้นของเน็ตเวิร์ก (Network Configuration)	149
การรักษาความปลอดภัยของโหนดของคุณ	153
ความปลอดภัยของระบบปฏิบัติการ	154
การเข้าถึงโหนด	155

การสำรองข้อมูลของโหนดและแซนแนล	156
ความเสี่ยงของกระเป๋าเงินแบบเชื่อมต่อออนไลน์ (Hot Wallet Risk)	158
การกวาดเงินถุง (Sweeping Funds)	159
เวลาทำงานและความพร้อมใช้งานของ Lightning Node	162
การยอมรับข้อผิดพลาดและการทำให้เป็นอัตโนมัติ	162
การตรวจสอบความพร้อมใช้งานของโหนด (Monitoring Node)	163
การตรวจสอบโดยบุคคลภายนอก (Watchtower)	164
การจัดการแซนแนล	165
การเปิดแซนแนลขาออก (Outbound Channels)	166
การได้รับสภาพคล่องขาเข้า (Inbound Liquidity)	170
การปิดแซนแนล (Closing Channels)	171
การปรับสมดุลแซนแนล (Rebalancing Channels)	171
ค่าธรรมเนียมการใช้เส้นทาง (Routing Fees)	173
การจัดการโหนด (Node Management)	174
Ride The Lightning	174
lndmon	175
ThunderHub	175
สรุปประจำบท	175
Part II ไลต์นิงเน็ตเวิร์กโดยละเอียด	176
CHAPTER 06 โครงสร้างสถาปัตยกรรมของไลต์นิงเน็ตเวิร์ก	177
ชุดโพรโทคอลของ Lightning Network	177
Lightning โดยรายละเอียด	179
CHAPTER 07 แซนแนลชำระเงิน	181
วิธีต่างๆ ในการใช้ระบบบิตคอยน์	182
ความเป็นเจ้าของและการควบคุมระบบบิตคอยน์	183
ความหลากหลายของการเป็นเจ้าของ (ที่เป็นอิสระ) และ Multisig	184
ความเป็นเจ้าของร่วมกันโดยไม่มี การควบคุมที่เป็นอิสระ	184
การป้องกันระบบบิตคอยน์ถูกล็อคและนำมาใช้จ่ายไม่ได้	184
การสร้างแซนแนลชำระเงิน	185
กุญแจส่วนตัวและสาธารณะของโหนด (Node Private and Public Keys)	185
ที่อยู่เน็ตเวิร์กของโหนด (Node Network Address)	186
ตัวระบุโหนด (Node Identifiers)	186
การเชื่อมต่อโหนดในฐานะ Peer โดยตรง (Direct Peers)	187
การสร้างแซนแนล	187
Peer Protocol สำหรับการจัดการแซนแนล	188
การรับส่งของข้อความการสร้างแซนแนล	188
ธุรกรรมฝากเงิน	192

การสร้างที่อยู่แบบหลายลายเซ็น	193
การสร้างธุรกรรมฝากเงิน	193
การถือธุรกรรมที่ลงนามแล้วแต่ไม่มีการประกาศออกไป	194
การคืนเงินก่อนการฝากเงิน	194
การสร้างธุรกรรมการคืนเงินที่กำหนดไว้ล่วงหน้า	195
การทำธุรกรรมต่อกันโดยไม่ประกาศออกไป	195
การแก้ปัญหาคาการเปลี่ยนแปลงได้	196
การประกาศธุรกรรมฝากเงิน	199
การส่งการชำระเงินผ่านแซนเนล	199
การแบ่งยอดเงินคงเหลือ	199
พันธสัญญาที่แข่งขันกัน	201
การถูกรีดด้วยธุรกรรมพันธสัญญาฉบับก่อนหน้า	201
การเพิกถอนธุรกรรมพันธสัญญาฉบับก่อนหน้า	202
ธุรกรรมพันธสัญญาที่ไม่สมมาตร	202
การใช้จ่ายที่ถูกหน่วงเวลา (Timelocked) to_self	203
กุญแจที่ใช้ในการเพิกถอน (Revocation Keys)	205
ธุรกรรมพันธสัญญา (Commitment Transaction)	205
การเปลี่ยนเป็นสถานะใหม่ของแซนเนล	208
ข้อความ commitment_signed	209
ข้อความ revoke_and_ack	210
การเพิกถอนและการทำพันธสัญญาใหม่	210
การถูกรีดและการลงโทษในทางปฏิบัติ	211
เงินทุนสำรองของแซนเนลเพื่อให้ยังอยู่ในเกม	214
การปิดแซนเนล (การปิดร่วมกัน)	214
ข้อความการปิดระบบ (Shutdown Message)	215
ข้อความ closing_signed	216
ธุรกรรมปิดแซนเนลร่วมกัน (Cooperative Close Transaction)	217
สรุปประจำบท	218
CHAPTER 08 การใช้เส้นทางบนเน็ตเวิร์กของแซนเนลชำระเงิน	219
การใช้เส้นทางชำระเงิน (Payment Channels)	220
การใช้เส้นทางกับการค้นหาเส้นทาง (Routing VS Pathfinding)	221
การสร้างเน็ตเวิร์กของแซนเนลชำระเงิน (Network of Payment Channels)	222
ตัวอย่างในชีวิตจริงของการใช้เส้นทาง	223
โปรโตคอลสร้างความยุติธรรม (Fairness Protocol)	229
การดำเนินการชำระเงินแบบ Atomic, ไม่ต้องเชื่อถือกัน และมีดีฮอป	230
ตัวอย่างการให้ทิปจากผู้ชม (อีกครั้ง)	231
การชำระบัญชีสัญญา HTLC แบบ On-Chain และ Off-chain	232

Hash Time-Locked Contracts (HTLC)	233
HTLC ในบิตคอยน์สคริปต์	234
Preimage ของการชำระหนี้และการยืนยันแฮช (Payment Preimage and Hash Verification)	235
การส่ง HTLC จากแอลิซไปยังบ๊อบ	236
การเผยแพร่ความลับแบบย้อนกลับ (Back-Propagatin)	237
การผูกลายเซ็น (Signature Binding) เพื่อป้องกันการโจรกรรม HTLC	239
การเพิ่มประสิทธิภาพของแฮช (Hash Optimization)	240
ความล้มเหลวของ HTLC ที่เกิดจากการร่วมมือกันและการหมดเวลา	242
การลดลงของ Timelock	244
สรุปประจำบท	244
CHAPTER 09 การดำเนินการของแซนเบลและการส่งต่อการชำระหนี้	245
การชำระหนี้แบบ Local (แซนเบลเดียว) เทียบกับ Routed (หลายแซนเบล)	246
การส่งต่อการชำระหนี้และการอัปเดตพันธสัญญาด้วยสัญญา HTLC	246
HTLC และการเคลื่อนที่ของข้อความพันธสัญญา	247
การส่งต่อการชำระหนี้ (Forwarding Payments) ด้วยสัญญา HTLC	247
การเพิ่มสัญญา HTLC	248
ข้อความ update_add_HTLC	248
HTLC ในธุรกรรมพันธสัญญา (Commitment Transactions)	249
พันธสัญญาใหม่ด้วยเอาต์พุต HTLC	251
แอลิซทำการผูกมัด (Alice Commits)	251
บ๊อบรับรู้ถึงพันธสัญญาใหม่ และเพิกถอนพันธสัญญาก่อนหน้า	253
บ๊อบทำการผูกมัด	255
HTLC หลายๆ สัญญา	256
การปฏิบัติตามสัญญา HTLC	257
การเผยแพร่สัญญา HTLC	257
ได้นำปฏิบัติตามสัญญา HTLC กับซาน	257
บ๊อบชำระหนี้ตามสัญญา HTLC กับแอลิซ	259
การนำสัญญา HTLC ออกไปเนื่องจากข้อผิดพลาดหรือการหมดอายุ	263
การชำระหนี้แบบ Local	263
สรุปประจำบท	264
CHAPTER 10 การใช้เส้นทางแบบ Onion	265
ตัวอย่างในชีวิตจริงของการใช้เส้นทางแบบ Onion	266
การเลือกเส้นทาง (Path)	266
การสร้างเลเยอร์ต่างๆ	267
การลอกเลเยอร์ต่างๆ	269

ความรู้เบื้องต้นเกี่ยวกับการใช้เส้นทางแบบ Onion ของสัญญา HTLC	270
แอลิซเลือกเส้นทาง	270
แอลิซสร้างเพย์โหนด	272
การสร้างกุญแจ	276
การห่อคลุมเลเยอร์ของ onion	280
Onion ที่มีความยาวคงที่	280
ขั้นตอนการห่อคลุมเลเยอร์ของ Onion	282
การห่อคลุมฮอปเพย์โหนดของดิน่า	283
การห่อคลุมฮอปเพย์โหนดของซ่าน	287
การห่อคลุมฮอปเพย์โหนดของบ๊อบ	288
แพ็กเก็ต Onion สุดท้าย	289
การส่ง Onion	289
ข้อความ update_add_htlc	289
แอลิซส่ง Onion ไปยังบ๊อบ	290
บ๊อบตรวจสอบ Onion	290
บ๊อบสร้างตัวเต็มเต็ม	291
บ๊อบทำให้ฮอปเพย์โหนดของเขาหายสับสน (De-obfuscate)	291
บ๊อบแยก HMAC ภายนอกออกสำหรับฮอปถัดไป	292
บ๊อบนำเพย์โหนดของเขาออก และเลื่อน Onion ไปข้างหน้า	292
บ๊อบสร้างแพ็กเก็ต Onion ใหม่	293
บ๊อบตรวจสอบยืนยันรายละเอียดของสัญญา HTLC	294
บ๊อบส่งข้อความ update_add_htlc ไปยังซ่าน	294
ซ่านส่งต่อ Onion	295
ดิน่าได้รับเพย์โหนดสุดท้าย	295
การแจ้งกลับข้อผิดพลาด	296
ข้อความแสดงความล้มเหลว	297
การชำระเงินที่เกิดขึ้นเองแบบ Keysend	300
บันทึก Onion TLV แบบกำหนดเอง	301
การส่งและการรับการชำระเงินแบบ keysend	301
Keysend และบันทึกแบบกำหนดเองในแอปพลิเคชันไลต์นิง	302
สรุปประจำวัน	302
CHAPTER 11 การซุ่มซิบและกราฟของแชนเนล	303
การค้นพบ Peer	306
การบูตสแตรปแบบ P2P (P2P Bootstrapping)	306
การบูตสแตรป DNS (DNS Bootstrapping)	307
ตัวเลือกในการสอบถามบันทึก SRV (SRV Query Options)	311
กราฟของแชนเนล (The Channel Graph)	312
กราฟที่ถูกกำหนดทิศทาง (Directed Graph)	313

ข้อความโปรโตคอลการซุบซิบ (Gossip Protocol Messages)	313
ข้อความ node_announcement	314
ข้อความ channel_announcement	316
ข้อความ channel_update	321
การดูแลรักษากราฟของแชนเนลอย่างต่อเนื่อง	322
สรุปประจำบท	323
CHAPTER 12 การค้นหาเส้นทางและการส่งการชำระเงิน	325
การค้นหาเส้นทางในชุดโปรโตคอลของ Lightning Network	325
มาตรฐาน BOLT หายไปไหน	326
ปัญหาที่ต้องถูกแก้ไขในการค้นหาเส้นทาง	326
การเลือกเส้นทางที่ดีที่สุด	327
การค้นหาเส้นทางในคณิตศาสตร์และวิทยาการคอมพิวเตอร์	328
ความจุ ยอดเงินคงเหลือ และสภาพคล่อง	328
ความไม่แน่นอนของยอดเงินคงเหลือ	329
ความซับซ้อนในการค้นหาเส้นทาง	330
การแก้ปัญหาแบบพื้นฐาน	331
กระบวนการในการค้นหาเส้นทางและการส่งการชำระเงิน	331
การสร้างกราฟของแชนเนล	332
ความไม่แน่นอนและความน่าจะเป็นของสภาพคล่อง	336
ค่าธรรมเนียมและตัวชี้วัดอื่นๆ ของแชนเนล	337
การหาเส้นทางที่เป็นตัวเลือก	339
การส่งการชำระเงิน (อุปการลองผิดลองถูก Trial-and-Error Loop)	340
ความพยายามครั้งแรก (เส้นทาง #1)	340
ความพยายามครั้งที่สอง (เส้นทาง #4)	341
การชำระเงินแบบหลายส่วน (Multipart Payments, MPP)	342
การใช้ MPP	343
การลองผิดลองถูกหลายรอบ	345
สรุปประจำบท	346
CHAPTER 13 การกำหนดโครงสร้างและความสามารถในการต่อขยาย	347
เลย์เออร์การส่งข้อความในชุดโปรโตคอลของ Lightning Network	347
การกำหนดโครงสร้างสายข้อความ (Wire Framing)	348
การกำหนดโครงสร้างสายข้อความในระดับสูง	348
การเข้ารหัสประเภทข้อความ (Type Encoding)	349
ส่วนขยายของข้อความ Type-Length-Value (TLV)	350
รูปแบบของข้อความ Protocol Buffer	351
ความเข้ากันได้แบบไปข้างหน้าและแบบย้อนกลับ	351

รูปแบบ Type-Length-Value (TLV)	352
การเข้ารหัสจำนวนเต็มแบบ BigInteger	353
ข้อจำกัดของการเข้ารหัส TLV	353
การเข้ารหัส TLV ตามหลักการ	354
มีตูล์เล่นและความสามารถในการต่อขยายโปรโตคอล	354
มีตูล์เล่นที่เป็นกลไกการค้นพบการอัปเดต	355
TLV สำหรับความเข้ากันได้แบบไปข้างหน้าและแบบย้อนกลับ	356
การจำแนกกลไกการอัปเดต	356
การอัปเดตในระดับการสร้างเซต	358
สรุปประจำบท	358
CHAPTER 14 การส่งข้อความที่ถูกเข้ารหัสของไลต์นิง	359
การส่งที่ถูกเข้ารหัสในชุดโปรโตคอลของ Lightning Network	359
บทนำ	360
กราฟของเซตในฐานโครงสร้างพื้นฐานของทฤษฎีกราฟแบบกระจายศูนย์	360
สาเหตุที่ไม่ใช้ TLS	361
โครงสร้างของ Noise Protocol	362
รายละเอียดการส่งข้อความที่ถูกเข้ารหัสของไลต์นิง	362
Noise_XK การทำความรู้จักกันด้วย Noise Protocol	363
สัญลักษณ์ของวิธีการทำความรู้จักกันและการทำงานของโปรโตคอล	363
ภาพรวมในระดับสูง	363
การทำความรู้จักกันในสามบทสนทนา (Three Acts)	365
สรุปประจำบท	375
CHAPTER 15 คำขอชำระเงินไลต์นิง	377
Invoice ในชุดโปรโตคอลของ Lightning Network	377
บทนำ	378
คำขอชำระเงินแบบไลต์นิง (Lightning Payment Requests) กับที่อยู่บิตคอยน์ (Bitcoin Address)	378
BOLT #11 การจัดเรียงลำดับและการตีความคำขอชำระเงิน	379
การเข้ารหัสคำขอชำระเงินในทางปฏิบัติ	379
คำนำหน้าที่สามารถอ่านและเข้าใจได้	379
bech32 และส่วนข้อมูล (Data Segment)	380
สรุปประจำบท	383
CHAPTER 16 ความปลอดภัยและความเป็นส่วนตัวของไลต์นิงเน็ตเวิร์ก	385
ความสำคัญของความเป็นส่วนตัว	385
นิยามของความเป็นส่วนตัว	385
กระบวนการในการประเมินความเป็นส่วนตัว (Evaluate Privacy)	386
เซตของภาวะนิรนาม (Anonymity Set)	388
ความแตกต่างระหว่าง Lightning Network และ Bitcoin เกี่ยวกับความเป็นส่วนตัว	389

การโจมตีบนโหนด	390
การสังเกตการณ์จำนวนเงินในการชำระหนี้	391
การเชื่อมโยงผู้ส่งและผู้รับ	391
การเปิดเผยยอดเงินคงเหลือของแชนแนล (การสืบสวน)	393
การปฏิเสธการให้บริการ (Denial of Service, DoS)	395
การทำให้พันธสัญญาติดขัด (Commitment Jamming)	397
การล๊อคสภาพคล่องของแชนแนล (Channel Liquidity Lockup)	398
การลบภาวะนิรนามแบบข้ามเลเยอร์	398
การรวมกลุ่มของบิตคอยน์ออนทึ่แบบ On-chain	399
การรวมกลุ่มของโหนดโหนดแบบ Off-chain	400
การเชื่อมโยงแบบข้ามเลเยอร์ของโหนดโหนด และกลุ่มบิตคอยน์ออนทึ่	401
โหนดกราฟ (Lightning Graph)	401
รูปแบบของโหนดกราฟในความเป็นจริง	402
การรวมศูนย์บน Lightning Network	405
แรงจูงใจทางเศรษฐกิจและโครงสร้างของกราฟ	405
คำแนะนำในทางปฏิบัติสำหรับผู้ใช้ในการปกป้องความเป็นส่วนตัว	406
แชนแนลที่ไม่ได้ถูกประกาศ (Unannounced Channels)	406
ข้อพิจารณาในการใช้เส้นทาง	407
การยอมรับแชนแนล	408
สรุปประจำบท	409
แหล่งอ้างอิงและศึกษาเพิ่มเติม	410
CHAPTER 17 บทสรุป	411
นวัตกรรมแบบกระจายศูนย์และอะซิงโครนัส	411
นวัตกรรมของบิตคอยน์โพรโทคอลและบิตคอยน์สคริปต์	412
นวัตกรรมสำหรับโหนดโหนดโพรโทคอล	413
ความสามารถในการต่อขยายแบบ TLV	413
การสร้างแชนแนลการชำระหนี้	413
ลูกเล่นแบบต้นทางถึงปลายทางที่เลือกได้โดยสมัครใจ	414
แอปพลิเคชันโหนด (LApp)	415
เมื่อพร้อมแล้วก็เริ่มต้นได้เลย	415
ภาคผนวก A การทบทวนพื้นฐานของบิตคอยน์	417
ภาคผนวก B การติดตั้งและการใช้งาน Docker ขั้นพื้นฐาน	439
ภาคผนวก C ข้อความใน Wire Protocol	443
ภาคผนวก D ข้อต้องทราบเกี่ยวกับที่มาและลิขสิทธิ์	461
อภิธานศัพท์	463



PART I

ทำความเข้าใจกับไลต์นิงเน็ตเวิร์ก

(Understanding the Lightning Network)

ภาพรวมของ Lightning Network ซึ่งเหมาะกับผู้สนใจที่จะทำความเข้าใจ
ในหลักการพื้นฐาน และวิธีการใช้งาน Lightning Network



CHAPTER 01

บทนำ

ยินดีต้อนรับสู่ Mastering the Lightning Network!

ไลต์นิงเน็ตเวิร์ก (Lightning Network) ซึ่งมักถูกเรียกสั้นๆ ว่า LN กำลังเปลี่ยนแปลงวิธีที่ผู้คนใช้แลกเปลี่ยนมูลค่าต่างๆ ผ่านช่องทางออนไลน์ และนับเป็นหนึ่งในความก้าวหน้าที่น่าตื่นตาตื่นใจที่สุดในประวัติศาสตร์ของบิตคอยน์ (Bitcoin) สำหรับปี 2021 ซึ่งเป็นปีปัจจุบันนั้น ไลต์นิงเน็ตเวิร์กยังคงอยู่ในระยะเริ่มต้น ไลต์นิงเน็ตเวิร์กเป็นโพรโทคอลในการใช้บิตคอยน์ที่ชาญฉลาดและใช้ได้จริง โดยเป็นเทคโนโลยีในระดับเลเยอร์ที่สองบนบิตคอยน์บล็อกเชน

แนวคิดเรื่องไลต์นิงเน็ตเวิร์ก ถูกนำเสนอขึ้นในปี 2015 และมีการเปิดตัวใช้เป็นครั้งแรกในปี 2018 ณ ปี 2021 นั้นเรายังอยู่ในแค่ช่วงเริ่มต้นที่จะเห็นโอกาสในการที่ไลต์นิงเน็ตเวิร์กจะทำให้การใช้บิตคอยน์มีความเป็นส่วนตัว มีความรวดเร็ว และมีความแพร่หลายมากขึ้น ผู้อ่านที่เข้าใจหลักการสำคัญของไลต์นิงเน็ตเวิร์กจะสามารถกำหนดอนาคตของมัน และสร้างโอกาสให้ตนเองได้

ผู้เขียนจะถือว่าผู้อ่านมีความรู้พื้นฐานเกี่ยวกับบิตคอยน์อยู่บ้าง อย่างไรก็ตาม ผู้อ่านที่ไม่มีความรู้มาก่อนเลยอาจไม่ต้องกังวลจนเกินไป เพราะผู้เขียนจะอธิบายหลักการต่างๆ ที่สำคัญของบิตคอยน์ที่จำเป็นต่อการทำความเข้าใจไลต์นิงเน็ตเวิร์กใน **ภาคผนวก A** ผู้อ่านที่ต้องการเรียนรู้เกี่ยวกับบิตคอยน์มากยิ่งขึ้นสามารถศึกษาเพิ่มเติมได้จากหนังสือ Mastering Bitcoin, 2nd Edition ที่เขียนโดย Andreas M. Antonopoulos (O'Reilly) โดยสามารถอ่านได้ฟรีในรูปแบบออนไลน์

แม้เนื้อหาส่วนใหญ่ของหนังสือเล่มนี้จะถูกเขียนมาสำหรับนักเขียนโปรแกรม แต่เนื้อหาบทแรกๆ นั้นถูกเขียนมาเพื่อให้ผู้อ่านในทุกกระดับสามารถเข้าใจได้แม้จะไม่มีความรู้ทางเทคนิค โดยในบทนี้ผู้เขียนจะเริ่มต้นจากการอธิบายนิยามต่างๆ รวมถึงการกล่าวถึงความเชื่อใจไว้วางใจ (Trust) และความสำคัญของมันในระบบต่างๆ ในส่วนท้ายจะเป็นการกล่าวถึงอดีต และอนาคตของไลต์นิงเน็ตเวิร์กเรามาเริ่มกันเลย

หนังสือ Mastering Bitcoin, 2nd Edition ฟรีในรูปแบบออนไลน์:

<https://github.com/bitcoinbook/bitcoinbook>

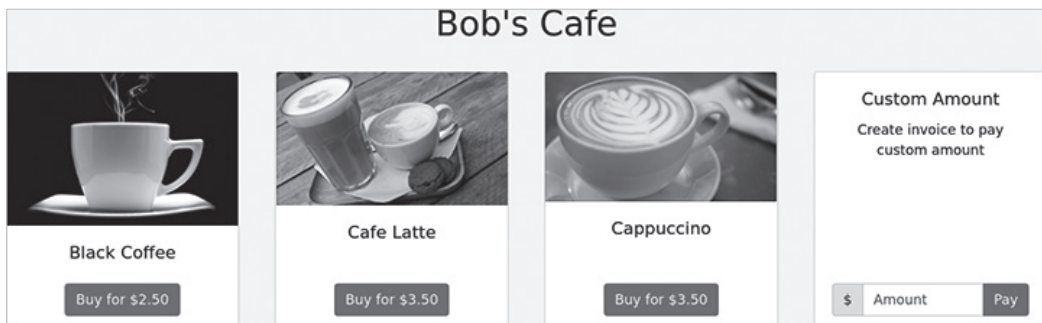
Bob's Cafe

บ๊อบมีแอปพลิเคชันระบบขายหน้าร้าน (Point-of-Sale, PoS) แบบง่ายๆ สำหรับรองรับลูกค้าที่ต้องการชำระเงินด้วยบิตคอยน์บนไลต์นิงเน็ตเวิร์ก ดังจะได้เห็นในบทถัดไป บ๊อบใช้ซอฟต์แวร์โอเพนซอร์สที่เป็นที่นิยมอย่าง BTCPay Server ที่มีส่วนประกอบทั้งหมดที่จำเป็นสำหรับธุรกิจพาณิชย์อิเล็กทรอนิกส์ (Ecommerce) หรือธุรกิจร้านค้าปลีก เช่น

- Bitcoin Node : บิตคอยน์โหนดที่ใช้ซอฟต์แวร์ Bitcoin Core
- Lightning Node : ไลต์นิงโหนดที่ใช้ซอฟต์แวร์ C-lightning
- PoS Application : แอปพลิเคชันระบบขายหน้าร้านสำหรับอุปกรณ์แท็บเล็ต

BTCPay Server ทำให้การติดตั้งซอฟต์แวร์ทั้งหมดที่จำเป็นง่ายขึ้น และทำให้การอัปโหลดรูปภาพและราคาสินค้า รวมถึงการเปิดตัวร้านเป็นไปอย่างรวดเร็วมากขึ้น

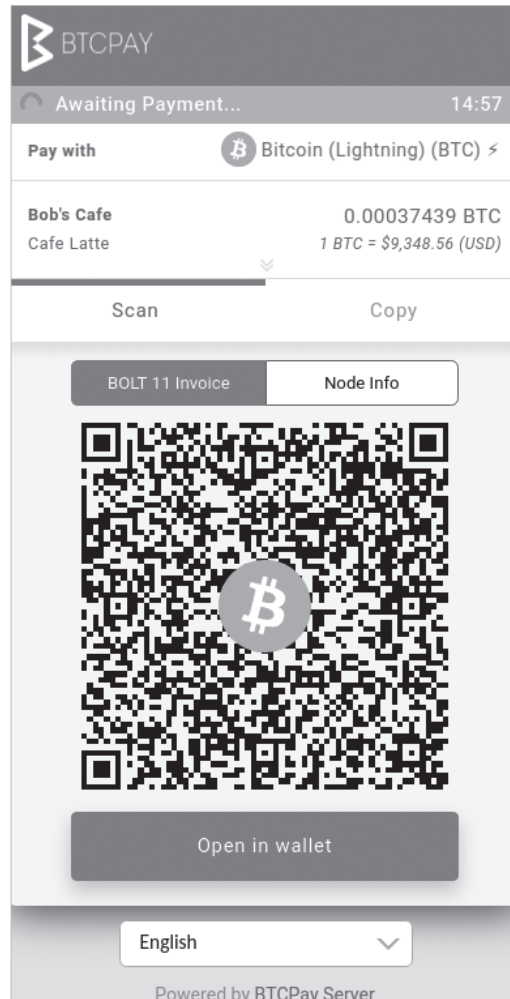
ณ จุดชำระเงินของ Bob's Cafe จะมีอุปกรณ์แท็บเล็ตที่แสดงให้เห็นภาพ ตามที่แสดงในภาพที่ 2-12



ภาพที่ 2-12 แอปพลิเคชันระบบขายหน้าร้านของบ๊อบ

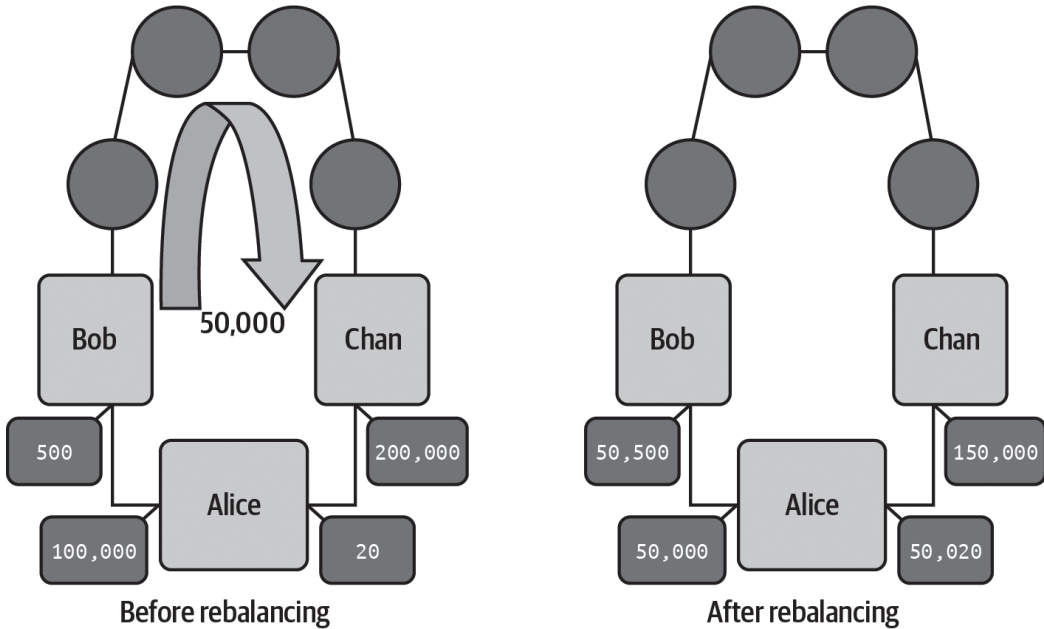
Lightning Invoice

แอลิซเลือก Cafe Latte จากตัวเลือกบนหน้าจอ และต่อมาได้เห็นใบแจ้งหนี้ “Lightning Invoice” (หรือที่รู้จักกันในชื่อ “Payment Request”) บนหน้าจอ ดังแสดงในภาพที่ 2-13



ภาพที่ 2-13 Lightning Invoice สำหรับ Latte ของแอลิซ

วิธีที่สามในการปรับสมดุลแชนเนล คือ การเจตนาสร้างเส้นทางแบบวงกลม (Circular Route) เพื่อชำระเงินจากโหนดของคุณกลับไปยังโหนดของคุณเองผ่าน Lightning Network การปรับสมดุลโดยวิธีนี้จะทำโดยการชำระเงินในแชนเนลที่มีความจุขนาดใหญ่ในด้านของคุณและจัดเรียงเส้นทางเพื่อให้มีการชำระเงินกลับมายังโหนดของคุณบนแชนเนลที่มีความจุขนาดใหญ่ในอีกด้านหนึ่งของแชนเนล ทั้งสองแชนเนลจะเกิดความสมดุลมากขึ้น คุณสามารถศึกษาตัวอย่างของกลยุทธ์ดังกล่าวได้ในภาพที่ 5-4



ภาพที่ 5-4 การปรับสมดุลโดยการสร้างเส้นทางแบบวงกลม (Circular Route Rebalancing)

การปรับสมดุลโดยการสร้างเส้นทางแบบวงกลม (Circular Rebalancing) สามารถทำได้บน Lightning Node ส่วนใหญ่ รวมถึงสามารถทำได้ด้วยการใช้บรรทัดคำสั่ง หรือผ่านหนึ่งในอินเทอร์เฟซที่ใช้การจัดการเว็บ เช่น Ride The Lightning (ดูหัวข้อ “Ride The Lightning” ในหน้า 174)

การปรับสมดุลแชนเนล (Channel Rebalancing) ยังถือเป็นเรื่องที่ซับซ้อน และเป็นประเด็นที่กำลังมีการศึกษาวิจัยอยู่ในปัจจุบัน โดยรายละเอียดเพิ่มเติมสามารถดูได้ในหัวข้อ “การปรับสมดุลแชนเนล (Rebalancing Channels)” ในหน้า 171



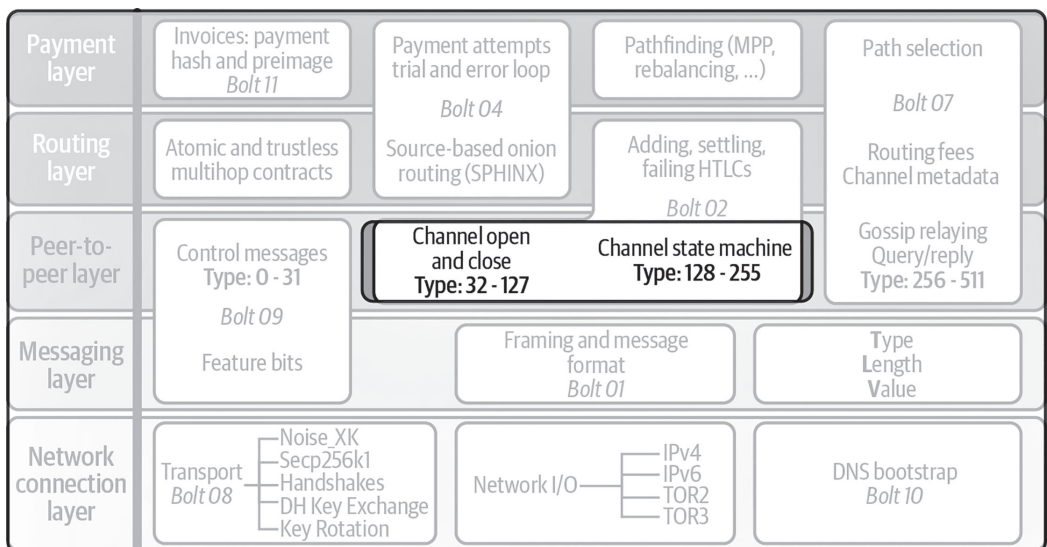
CHAPTER 07

แชแนลชำระเงิน

(Payment Channels)

ในบทนี้เราจะกล่าวลึกลงไปเกี่ยวกับแชแนลชำระเงิน รวมถึงวิธีที่มันถูกสร้างขึ้นมา โดยจะเริ่มจากการที่โหนดของเอลิซ (Alice's node) กำลังเปิดแชแนลไปสู่โหนดของบ๊อบ (Bob's node) ซึ่งเป็นตัวอย่างที่ต่อเนื่องมาจากส่วนต้นของหนังสือเล่มนี้

ข้อความที่ถูกแลกเปลี่ยนระหว่างโหนดของเอลิซและบ๊อบ จะถูกอธิบายไว้ในเอกสารมาตรฐาน “BOLT #2: Peer Protocol for Channel Management” ส่วนธุรกรรมที่สร้างจากโหนดของเอลิซและบ๊อบ จะถูกอธิบายไว้ในเอกสารมาตรฐาน “BOLT #3: Bitcoin Transaction and Script Formats” โดยในบทนี้เราจะเน้นเกี่ยวกับส่วน “Channel open and close” และ “Channel state machine” ของโครงสร้างสถาปัตยกรรมของไลต์นิงโพรโทคอล (Lightning Protocol Architecture) ดังที่ได้แสดงไว้ในส่วนกลาง (เลเยอร์ไรต์วกลง หรือ Peer-to-Peer Layer) ของภาพที่ 7-1



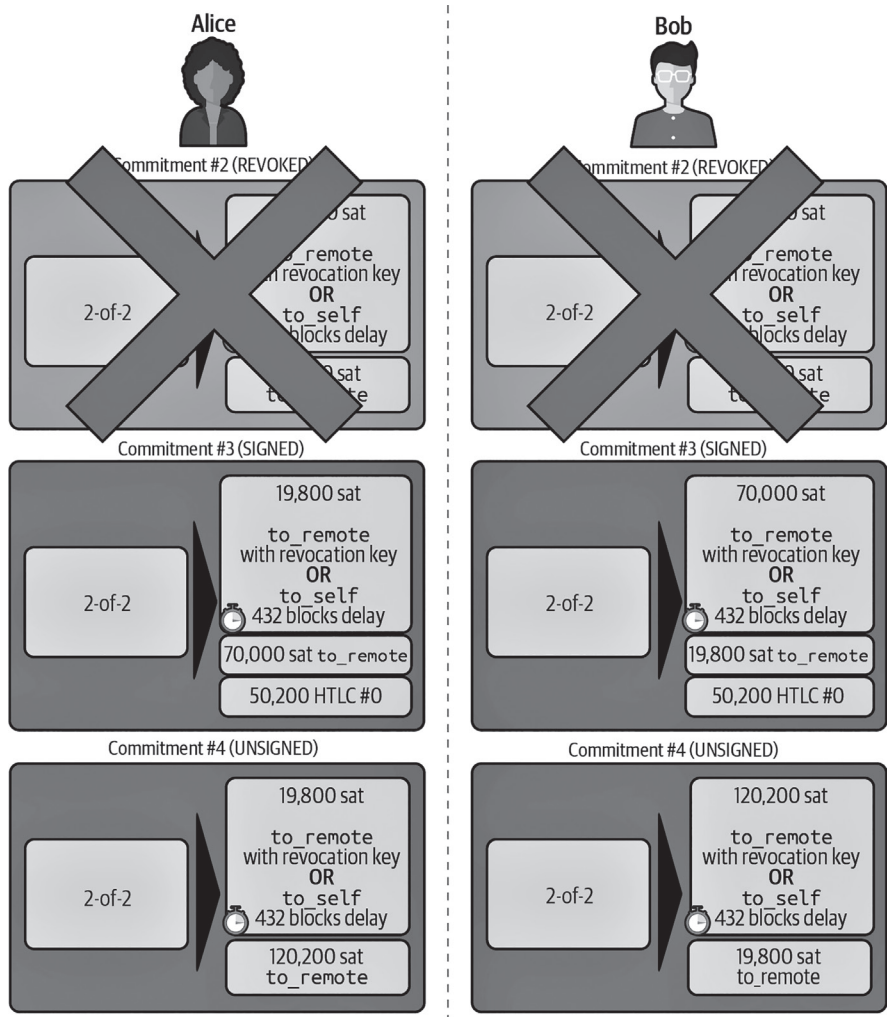
ภาพที่ 7-1 แชแนลชำระเงินในชุดไลต์นิงโพรโทคอล

Channel Management : <https://github.com/lightning/bolts/blob/master/02-peer-protocol.md>

Bitcoin Transaction and Script Formats :

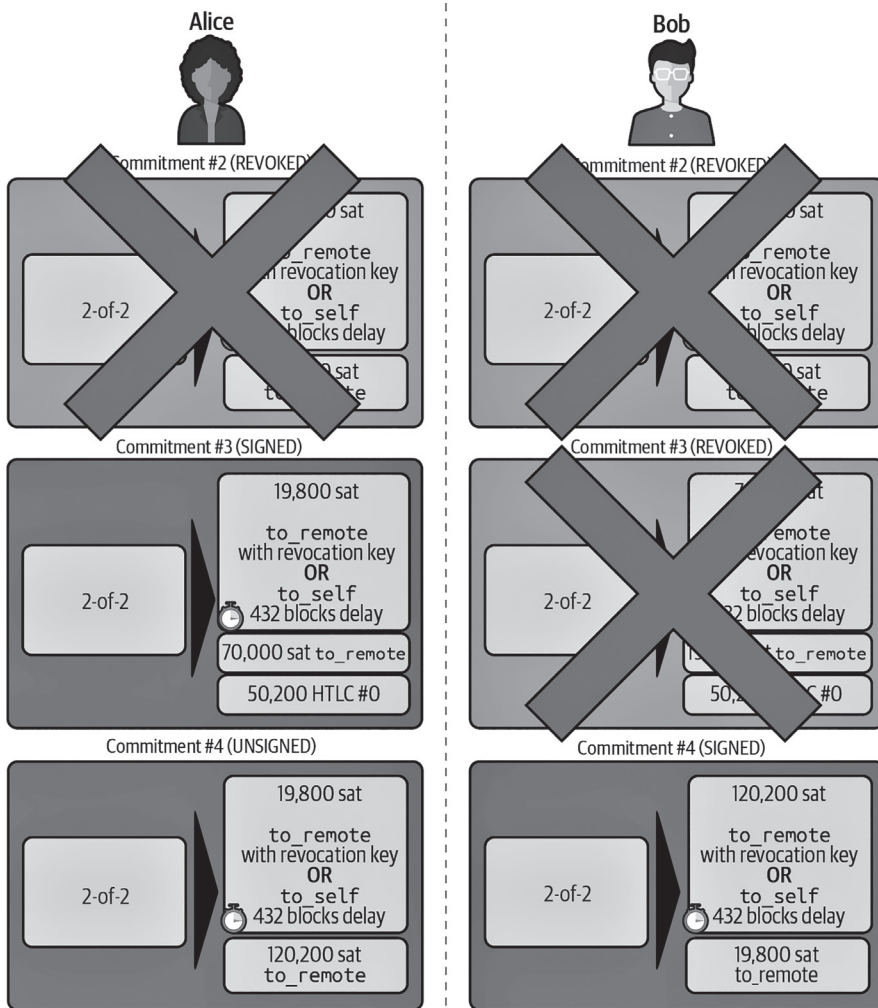
<https://github.com/lightning/bolts/blob/master/03-transactions.md>

พวกเขาสามารถสร้างพันธสัญญาใหม่ (Commitment #4) ดังที่แสดงในภาพที่ 9-12



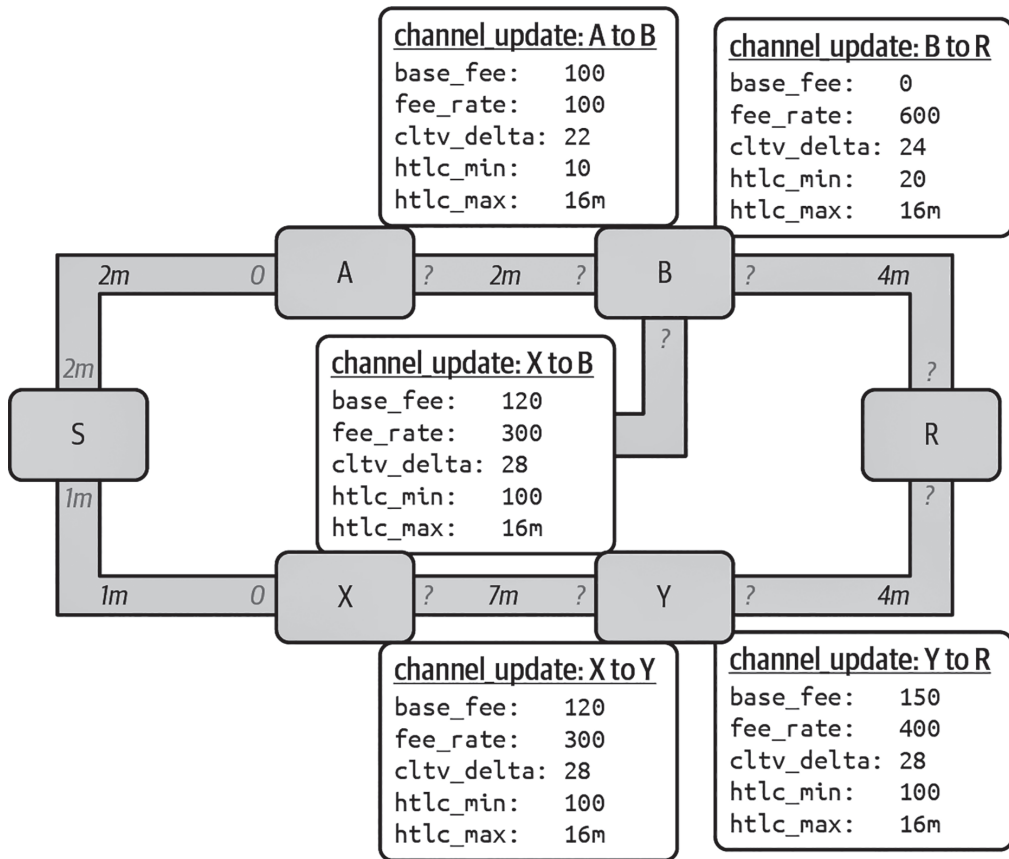
ภาพที่ 9-12 สัญญา HTLC ถูกนำออกไปและยอดเงินคงเหลือถูกอัปเดตในพันธสัญญาใหม่

ในขั้นตอนนี้ต่อไป พวกเขาจะทำพันธสัญญาและการเพิกถอนสองรอบ ก่อนอื่นแอ丽丝จะส่งข้อความ `commitment_signed` เพื่อลงนามในธุรกรรมพันธสัญญาใหม่ของบ๊อบ และบ๊อบจะตอบกลับด้วยข้อความ `revoid_and_ack` เพื่อเพิกถอนพันธสัญญาฉบับก่อนของเขา เมื่อบ๊อบได้เคลื่อนสถานะของแซนเบลไปข้างหน้าเรียบร้อยแล้ว พันธสัญญาจะมีลักษณะเหมือนที่ผู้อ่านเห็นในภาพที่ 9-13



ภาพที่ 9-13 แอลิซลงนามในธุรกรรมใหม่ของบ๊อบ และบ๊อบเพิกถอนธุรกรรมฉบับก่อน

และด้วยการอัปเดตนี้ แอลิซจะประกาศออกไปว่าเธอจะเรียกเก็บค่าธรรมเนียมเท่าใดในการให้ใช้เส้นทางในการส่งต่อสัญญา HTLC ไปยังบ็อบผ่านแชนเนลเฉพาะนั้น และบ็อบก็อาจประกาศการอัปเดตแชนเนล (ไม่ถูกแสดงในภาพนี้) ในทิศทางตรงกันข้ามโดยมีความคาดหวังค่าธรรมเนียมที่แตกต่างไปจากนี้ อย่างสิ้นเชิงก็ได้ โหนดใดๆ อาจส่งข้อความ `channel_update` ใหม่เพื่อเปลี่ยนความคาดหวังเกี่ยวกับค่าธรรมเนียมหรือ Timelock ได้ตลอดเวลา



ภาพที่ 12-6 ค่าธรรมเนียมของกราฟและตัวชี้วัดอื่นๆ ของแชนเนล

ข้อมูลเกี่ยวกับค่าธรรมเนียมและ Timelock มีความสำคัญมาก โดยไม่ใช่แค่เป็นเพียงตัวชี้วัดในการเลือกเส้นทางเท่านั้น ดังที่เราได้เห็นในบทที่ 10 ผู้ส่งจะต้องเพิ่มค่าธรรมเนียมและค่า Timelock (`cltv_expiry_delta`) ในแต่ละฮอปเพื่อสร้าง Onion กระบวนการคำนวณค่าธรรมเนียมเกิดขึ้นจากผู้รับไปยังผู้ส่งในแบบย้อนหลังไปตามเส้นทาง เนื่องจากแต่ละฮอปตัวกลางคาดหวังว่าจะมีสัญญา HTLC ขาเข้าที่มีจำนวนเงินและค่าการหน่วงเวลาหมดอายุที่สูงกว่าสัญญา HTLC ขาออกที่พวกเขาจะส่งไปยังฮอปถัดไป ตัวอย่างเช่น หากบ็อบต้องการได้รับค่าธรรมเนียม 1,000 Satoshi และเวลาหมดอายุของ Timelock Delta ที่ 30 Blocks เพื่อส่งการชำระเงินให้กับราซิด แอลิซก็ต้องเพิ่มจำนวนเงินและเวลาหมดอายุของ Timelock Delta นั้นไปยังสัญญา HTLC ของเธอด้วย

การส่งการชำระเงิน (อุปกรณ์ลองผิดลองถูก Trial-and-Error Loop)

โหนดของเซเลน่าเริ่มต้นอุปกรณ์ลองผิดลองถูกโดยการสร้างสัญญา HTLC สร้าง Onion และพยายามส่งการชำระเงิน สำหรับความพยายามแต่ละครั้งจะมีผลลัพธ์ที่เป็นไปได้ 3 แบบ ดังต่อไปนี้

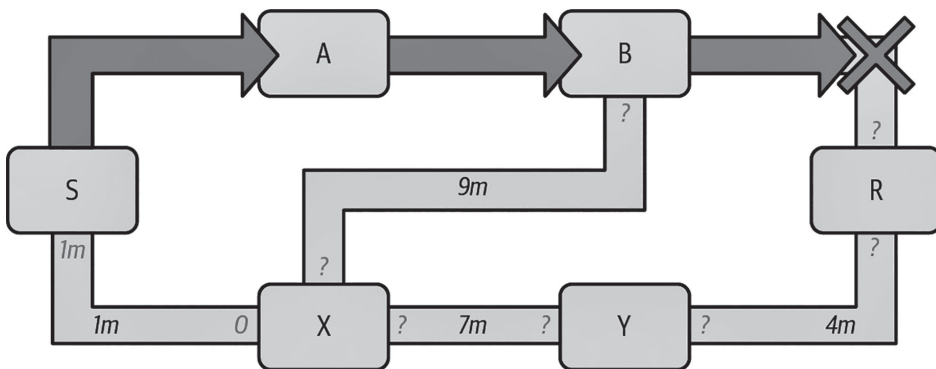
- ผลลัพธ์ที่สำเร็จ (`update_fulfill_htlc`)
- ข้อผิดพลาด (`update_fail_htlc`)
- การชำระเงินที่ติดขัดโดยไม่มีการตอบสนอง (ไม่สำเร็จหรือไม่ล้มเหลว)

หากการชำระเงินล้มเหลว เราสามารถลองอีกครั้งผ่านเส้นทางอื่นโดยการอัปเดตกราฟ (เปลี่ยนตัวชี้วัดของแชนเนล) และคำนวณเส้นทางอื่นใหม่

เราได้กล่าวถึงสิ่งที่เกิดขึ้นเมื่อการชำระเงินเกิดการติดขัด ในหัวข้อ “การชำระเงินที่ติดขัด (Stuck Payment)” ในหน้า 299 โดยรายละเอียดที่สำคัญ ได้แก่ การที่การชำระเงินที่ติดขัด ซึ่งนี่จะเป็นผลลัพธ์ที่แย่ที่สุด เนื่องจากเราไม่สามารถลองส่งอีกครั้งได้ด้วยสัญญา HTLC อื่นได้ เพราะทั้งสองการส่ง (การชำระเงินที่ติดขัดและการลองใหม่อีกครั้ง) อาจเสร็จสมบูรณ์ในที่สุดและทำให้เกิดการชำระเงินที่ซ้ำซ้อนได้

ความพยายามครั้งแรก (เส้นทาง #1)

เซเลน่าพยายามใช้เส้นทางแรก ($S \rightarrow A \rightarrow B \rightarrow R$) จากตัวเลือกข้างต้น โดยเธอได้สร้าง Onion และส่งมันไป แต่ได้รับรหัสแสดงความล้มเหลวจากโหนดของบ๊อบ โดยบ๊อบจะรายงานกลับมาถึงความล้มเหลวของแชนเนลแบบชั่วคราว (Temporary Channel Failure) ด้วยข้อความ `channel_update` ที่ระบุว่าแชนเนล $B \rightarrow R$ เป็นแชนเนลที่ไม่สามารถส่งต่อการชำระเงินได้ ความพยายามดังกล่าวถูกแสดงในภาพที่ 12-7



ภาพที่ 12-7 ความพยายามของเส้นทาง #1 เกิดความล้มเหลว



ภาคผนวก A

การทบทวนพื้นฐานของบิตคอยน์

(Bitcoin Fundamentals Review)

ไลต์นิงเน็ตเวิร์ก (Lightning Network) มีความสามารถในการทำงานได้บนหลายๆ บล็อกเชน แต่จะทำงานเป็นหลักอยู่บนบิตคอยน์บล็อกเชน เพื่อทำความเข้าใจไลต์นิงเน็ตเวิร์ก คุณจำเป็นต้องมีความเข้าใจพื้นฐานเกี่ยวกับบิตคอยน์ และองค์ประกอบของมันก่อน

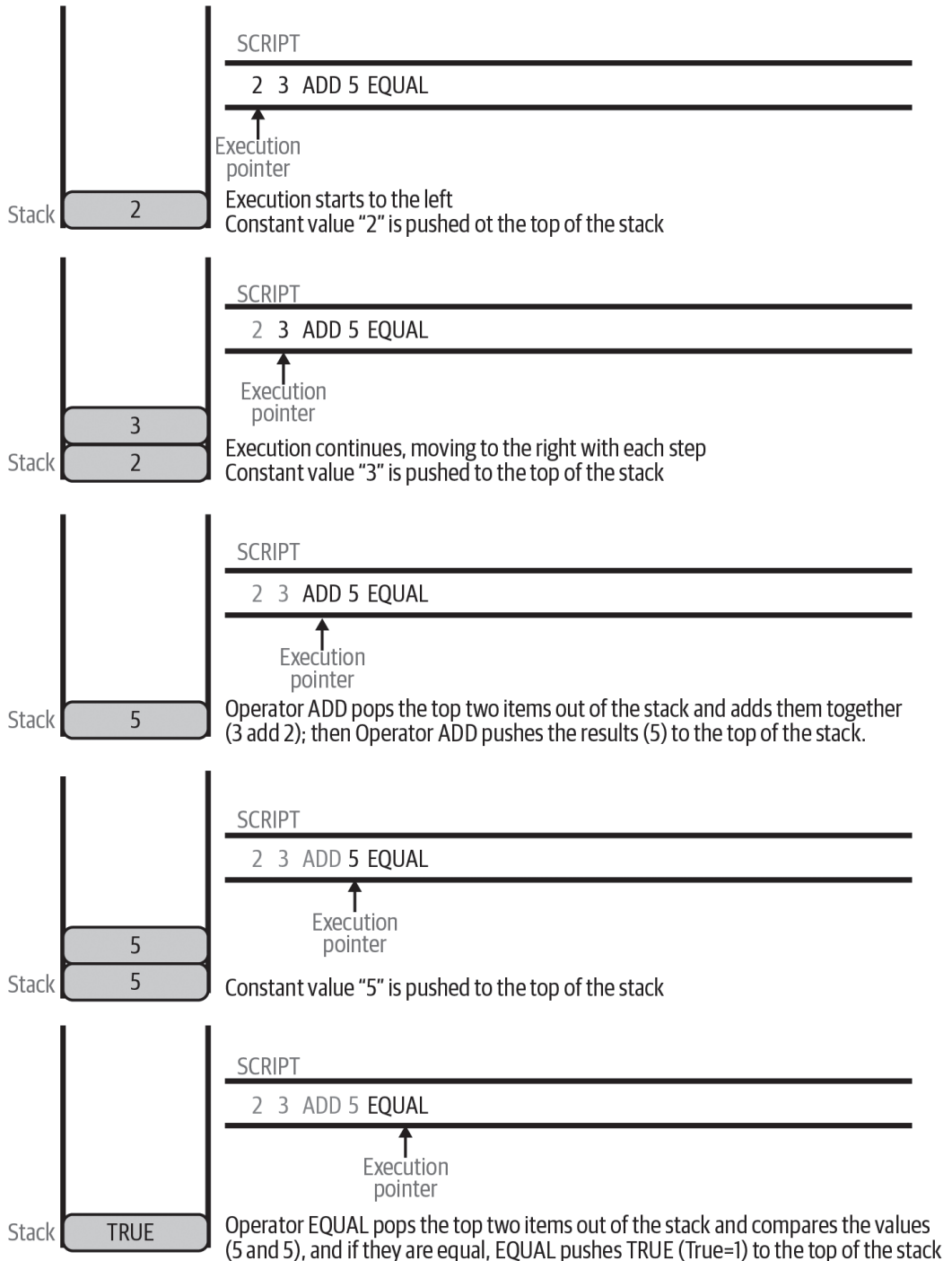
มีแหล่งข้อมูลที่มีประโยชน์จำนวนมากที่คุณสามารถใช้เพื่อเรียนรู้เพิ่มเติมเกี่ยวกับบิตคอยน์ รวมถึงหนังสือ **Mastering Bitcoin** ฉบับตีพิมพ์ครั้งที่ 2 โดย Andreas M. Antonopoulos ซึ่งคุณสามารถหาอ่านได้บน GitHub ภายใต้ลิขสิทธิ์แบบโอเพนซอร์ส (<https://github.com/bitcoinbook/bitcoinbook>) อย่างไรก็ตาม คุณไม่จำเป็นต้องอ่านหนังสือเล่มอื่นทั้งเล่มเพื่อเตรียมพร้อมในการอ่านหนังสือเล่มนี้ก็ได้

ในบทนี้ผู้เขียนได้รวบรวมแนวคิดที่สำคัญที่สุดที่คุณต้องรู้เกี่ยวกับบิตคอยน์ และอธิบายแนวคิดดังกล่าวในบริบทของไลต์นิงเน็ตเวิร์ก ด้วยวิธีนี้คุณจะได้เรียนรู้อย่างชัดเจนถึงสิ่งที่คุณจำเป็นต้องรู้เพื่อศึกษาไลต์นิงเน็ตเวิร์ก

บทนี้ประกอบด้วยแนวคิดที่สำคัญบางประการของระบบบิตคอยน์ ซึ่งได้แก่

- กฎและลายเซ็นดิจิทัล
- ฟังก์ชันแฮช
- โครงสร้างบิตคอยน์ และโครงสร้างของมัน
- การสร้างลูกโซ่ของธุรกรรมบิตคอยน์
- Outpoint ของธุรกรรม
- บิตคอยน์สคริปต์ รวมถึงสคริปต์สำหรับล็อก (Locking Script) และสคริปต์สำหรับปลดล็อก (Unlocking Script)
- สคริปต์สำหรับล็อกแบบพื้นฐาน
- สคริปต์สำหรับล็อกที่มีความซับซ้อนและมีเงื่อนไข
- Timelock

ในภาพที่ A-8 เราจะได้เห็นวิธีการทำงานของสคริปต์ดังกล่าว (จากซ้ายไปขวา)



ภาพที่ A-8 ตัวอย่างการทำงานของบิตคอยน์สคริปต์



ภาคผนวก C

ข้อความใน Wire Protocol

(Wire Protocol Messages)

ภาคผนวกนี้แสดงรายการของประเภทข้อความที่ถูกระบุขึ้นในปัจจุบันทั้งหมดที่ใช้ในไลต์นิงโปรโตคอลแบบ P2P นอกจากนี้ เรายังแสดงโครงสร้างของแต่ละข้อความ โดยการจัดกลุ่มข้อความเป็นกลุ่มตามการกระบวนกรของโปรโตคอล



ข้อความของไลต์นิงโปรโตคอลสามารถถูกต่อขยายได้และโครงสร้างของมันอาจมีการเปลี่ยนแปลงระหว่างการอัปเดตแบบทั่วทั้งเน็ตเวิร์ก หากต้องการทราบข้อมูลที่เชื่อถือได้ ผู้อ่านสามารถดูได้จากมาตรฐาน BOLT เวอร์ชันล่าสุดจากที่เก็บอยู่ในคลังข้อมูล Github Lightning-RFC (<https://github.com/lightningnetwork/lightning-rfc>)

ประเภทของข้อความ (Message Types)

ประเภทของข้อความที่ถูกระบุขึ้นในปัจจุบันถูกแสดงในตารางที่ C-1

ตารางที่ C-1 ประเภทของข้อความ

จำนวนเต็มระบุประเภท	ชื่อของข้อความ	หมวดหมู่
16	init	การสร้างการเชื่อมต่อ
17	error	การสื่อสารข้อผิดพลาด
18	ping	การทำงานอยู่ของการเชื่อมต่อ
19	pong	การทำงานอยู่ของการเชื่อมต่อ
32	open_channel	การฝากเงินเข้าแชนเนล
33	accept_channel	การฝากเงินเข้าแชนเนล
34	funding_created	การฝากเงินเข้าแชนเนล
35	funding_signed	การฝากเงินเข้าแชนเนล
36	funding_locked	การฝากเงินเข้าแชนเนลและการดำเนินการแชนเนล
38	shutdown	การปิดแชนเนล

จำนวนเต็มระบุประเภท	ชื่อของข้อความ	หมวดหมู่
39	closing_signed	การปิดแชนเนล
128	update_add_htlc	การดำเนินการแชนเนล
130	update_fulfill_htlc	การดำเนินการแชนเนล
131	update_fail_htlc	การดำเนินการแชนเนล
132	commit_sig	การดำเนินการแชนเนล
133	revoke_and_ack	การดำเนินการแชนเนล
134	update_fee	การดำเนินการแชนเนล
135	update_fail_malformed_htlc	การดำเนินการแชนเนล
136	channel_reestablish	การดำเนินการแชนเนล
256	channel_announcement	การประกาศแชนเนล
257	node_announcement	การประกาศแชนเนล
258	channel_update	การประกาศแชนเนล
259	announce_signatures	การประกาศแชนเนล
261	query_short_chan_ids	การชิงค์แชนเนลกราฟ
262	reply_short_chan_ids_end	การชิงค์แชนเนลกราฟ
263	query_channel_range	การชิงค์แชนเนลกราฟ
264	reply_channel_range	การชิงค์แชนเนลกราฟ
265	gossip_timestamp_range	การชิงค์แชนเนลกราฟ

ในตารางที่ C-1 เขตข้อมูลหมวดหมู่ ทำให้เราสามารถจัดหมวดหมู่ข้อความได้อย่างรวดเร็วตามฟังก์ชันการทำงานภายในโพรโทคอลเอง ในระดับสูง เราจะจัดข้อความไว้ในหนึ่งในแปดกลุ่ม (อาจมีมากกว่านี้) ได้แก่

การสร้างการเชื่อมต่อ (Connection Establishment)

ถูกส่งเมื่อมีการสร้างการเชื่อมต่อแบบ Peer ทุ Peer เป็นครั้งแรก ยังถูกใช้เพื่อเจรจาชุดของลูกเล่นที่ได้รับการรองรับจากการเชื่อมต่อใหม่

