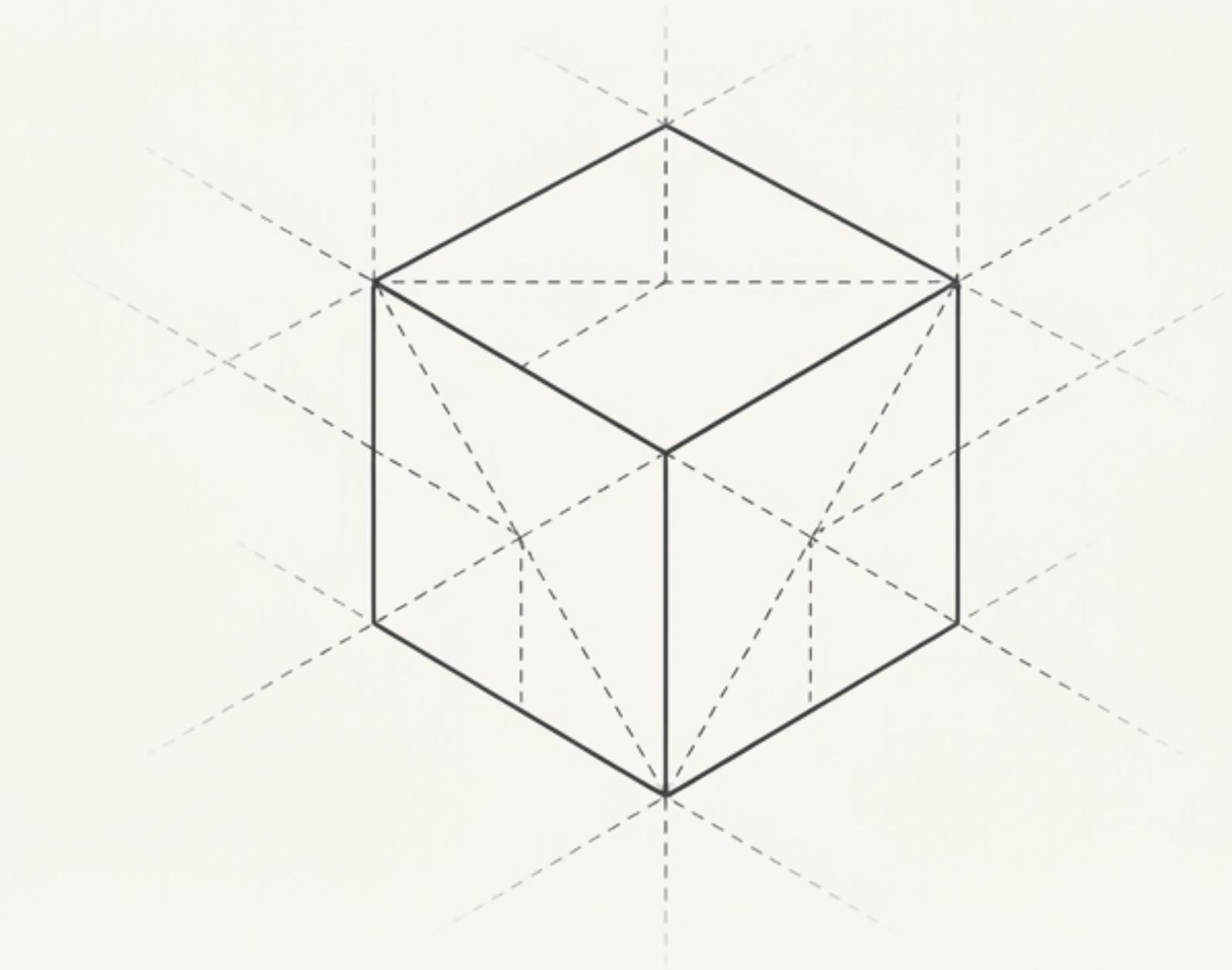


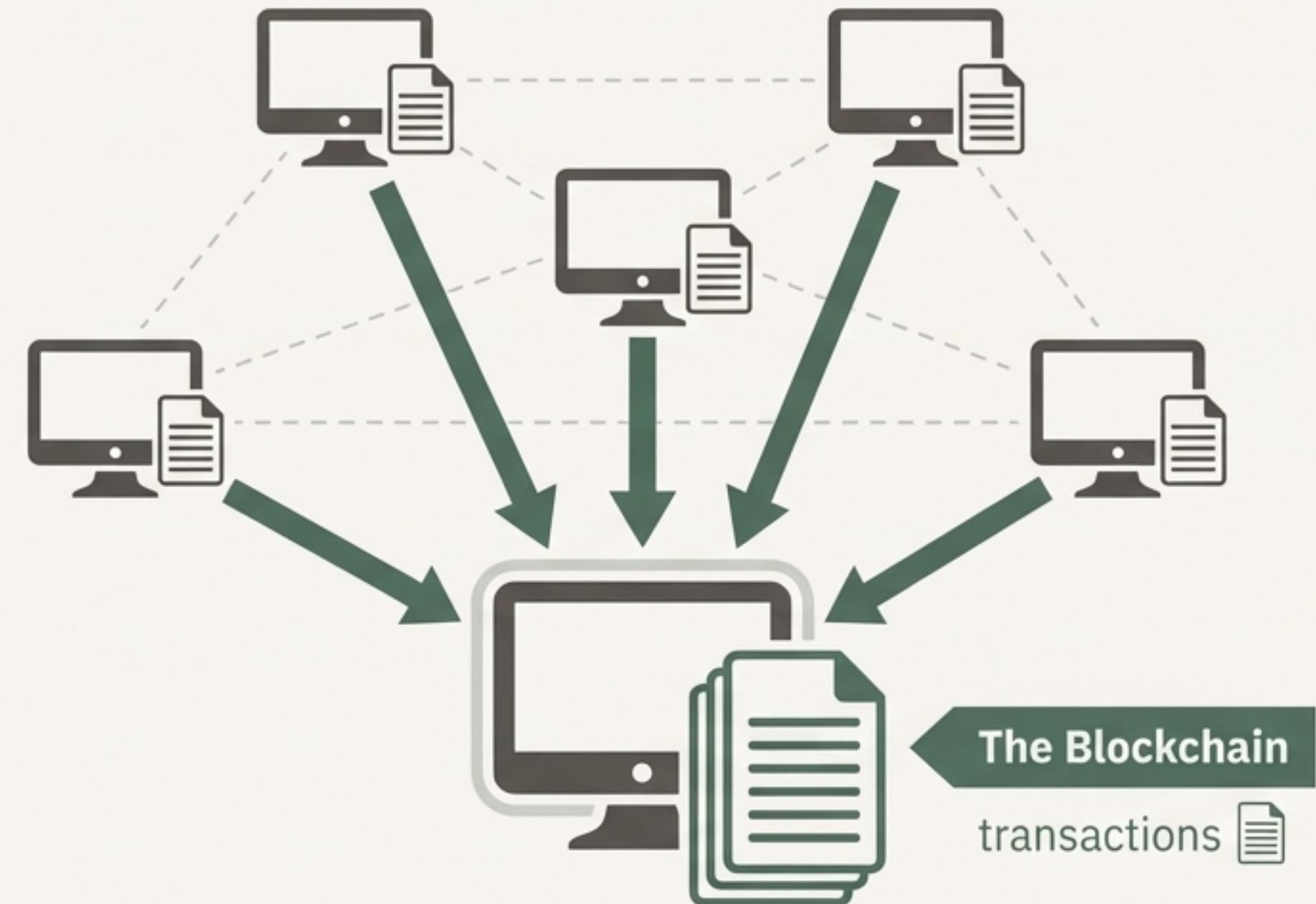
Bitcoin ทำงานอย่างไร

คำอธิบายฉบับสมบูรณ์สำหรับผู้เริ่มต้นที่อยากเข้าใจอย่างลึกซึ้ง



หัวใจของ Bitcoin คือโปรแกรมคอมพิวเตอร์ที่แชร์ไฟล์ร่วมกัน

- เมื่อคุณเปิดโปรแกรม Bitcoin มันจะเชื่อมต่อกับคอมพิวเตอร์เครื่องอื่น ๆ ที่ใช้โปรแกรมเดียวกัน
- เครือข่ายนี้จะเริ่มแชร์ไฟล์หนึ่งกับคุณ ซึ่งเรียกว่า **Blockchain**
- Blockchain ก็คือบัญชีสาธารณะ (Public Ledger) ที่บันทึกรายการธุกรรมทั้งหมด



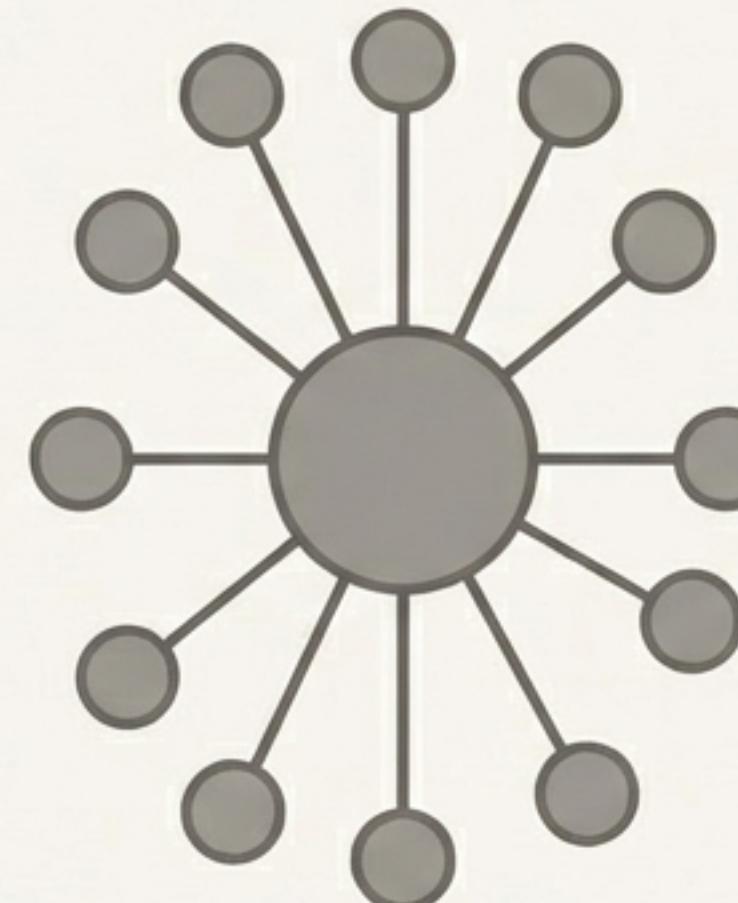
Bitcoin ถูกสร้างขึ้นเพื่อเป็นทางเลือกของระบบการเงินแบบรวมศูนย์

ในระบบปัจจุบัน ธนาคารขนาดใหญ่เพียงไม่กี่แห่งเป็นผู้ควบคุมการเงิน ทำให้เราต้อง ‘เชื่อใจ’ พวกเขา

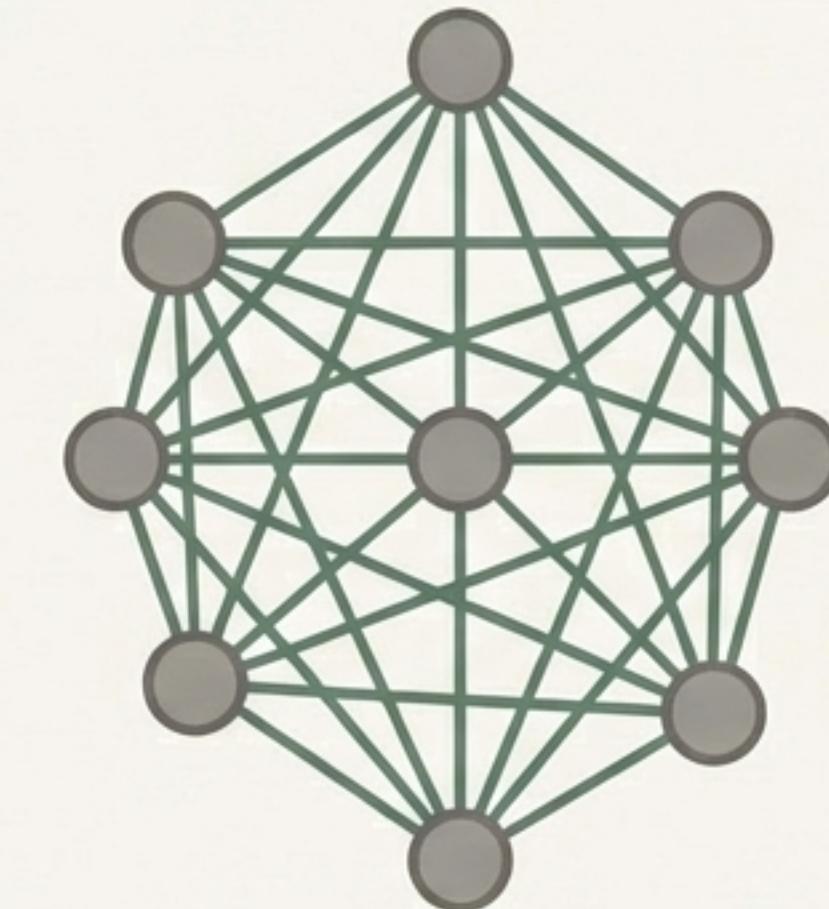
Bitcoin ถูกสร้างขึ้นโดยบุคคลนิรนาม ‘Satoshi Nakamoto’ หลังวิกฤตการเงินปี 2008 เพื่อสร้างระบบชำระเงินที่ไม่ต้องอาศัยตัวกลาง

“ธนาคารต้องได้รับความไว้วางใจให้ถือเงินของเราและโอนเงินทางอิเล็กทรอนิกส์ แต่พวกเขาลับปล่อยภัยในระบบทอกของฟองสบู่สินเชื่อโดยมีเงินสำรองเพียงเศษเสี้ยว” - Satoshi Nakamoto

Centralized



Decentralized

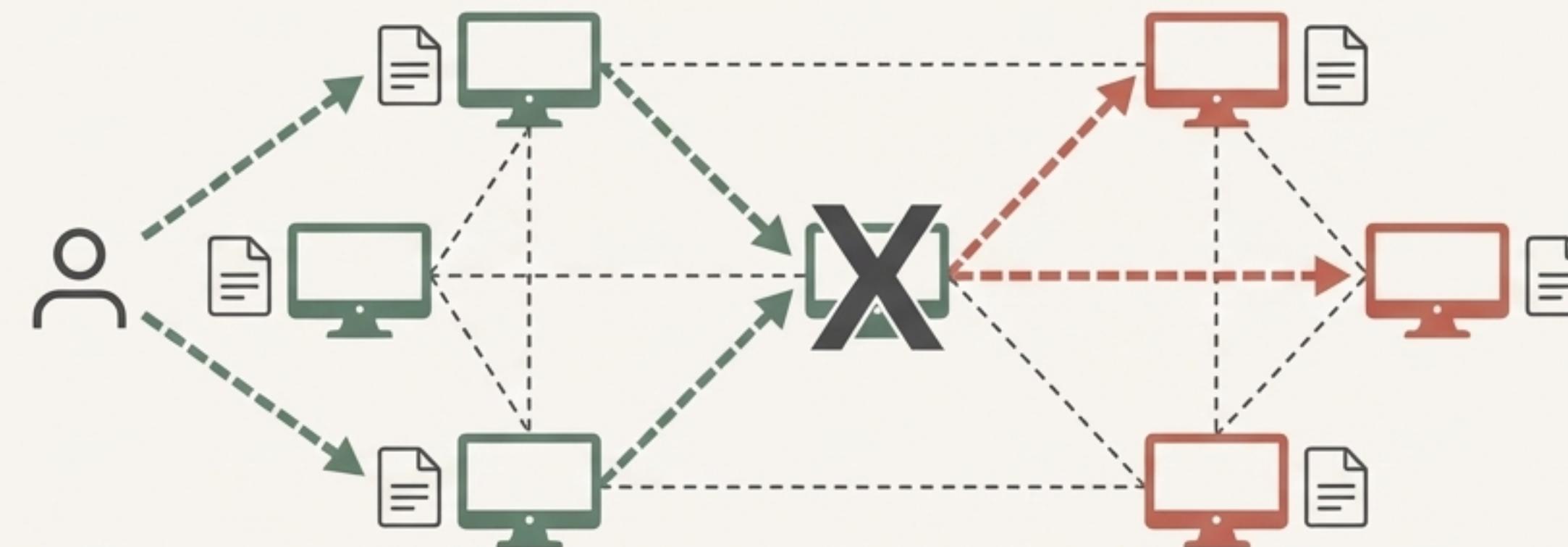


ความท้าทายที่สำคัญที่สุด: ปัญหาการใช้จ่ายซ้ำซ้อน (Double-Spend)

ในระบบที่ไม่มีศูนย์กลาง จะเกิดอะไรขึ้นถ้ามีคนสร้างสองธุรกรรมเพื่อใช้ ‘เหรียญดิจิทัลเหรียญเดียวกัน’ และส่งออกไปพร้อม ๆ กัน?

คอมพิวเตอร์บางเครื่องจะได้รับธุรกรรม A ก่อน ในขณะที่บางเครื่องได้รับธุรกรรม B ก่อน

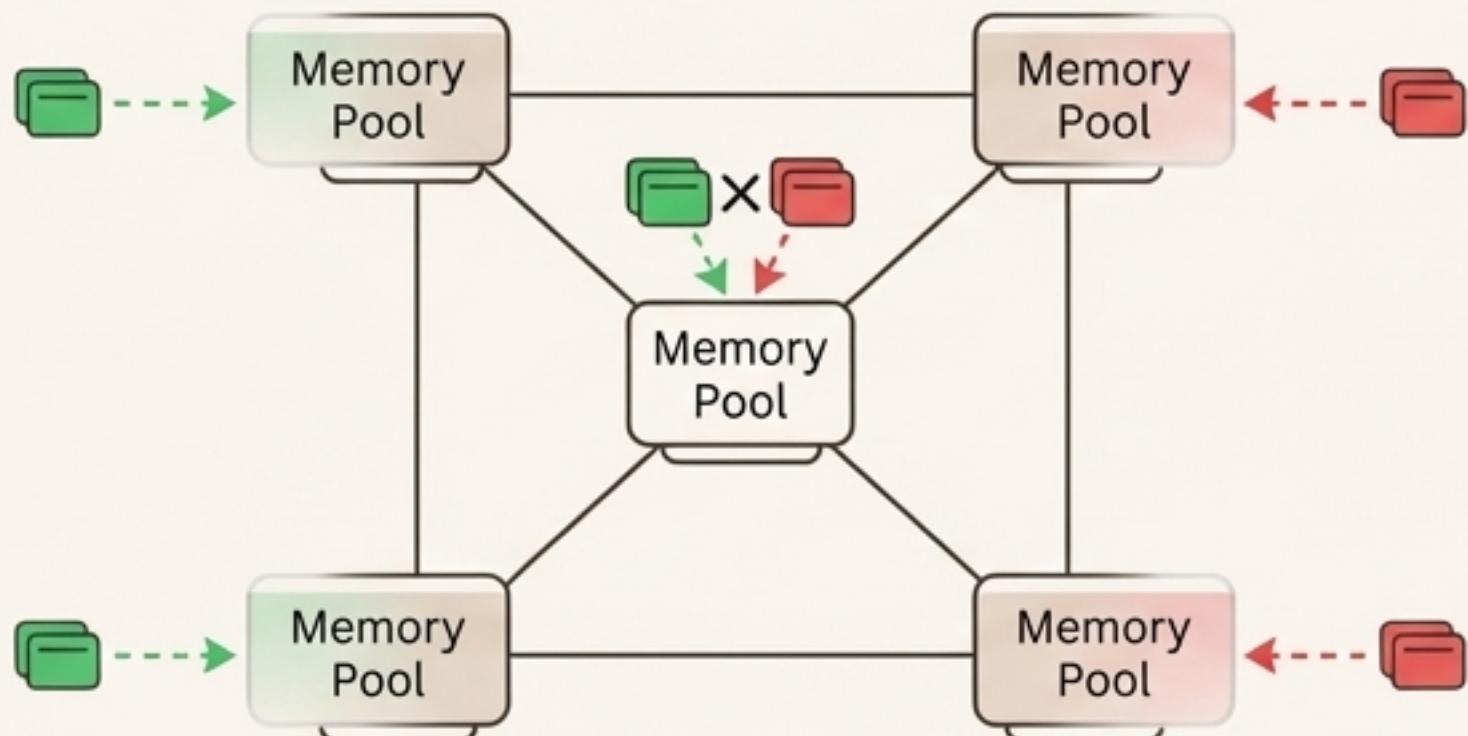
เครือข่ายจะรู้ได้อย่างไรว่าธุรกรรมไหนที่ ‘ถูกต้อง’ และเกิดขึ้นก่อน? นี่คือปัญหาหลักที่ต้องแก้ไข



วิธีแก้ปัญหาของ Bitcoin: สร้างกติกาเพื่อหาผู้ชนะเพียงหนึ่งเดียว

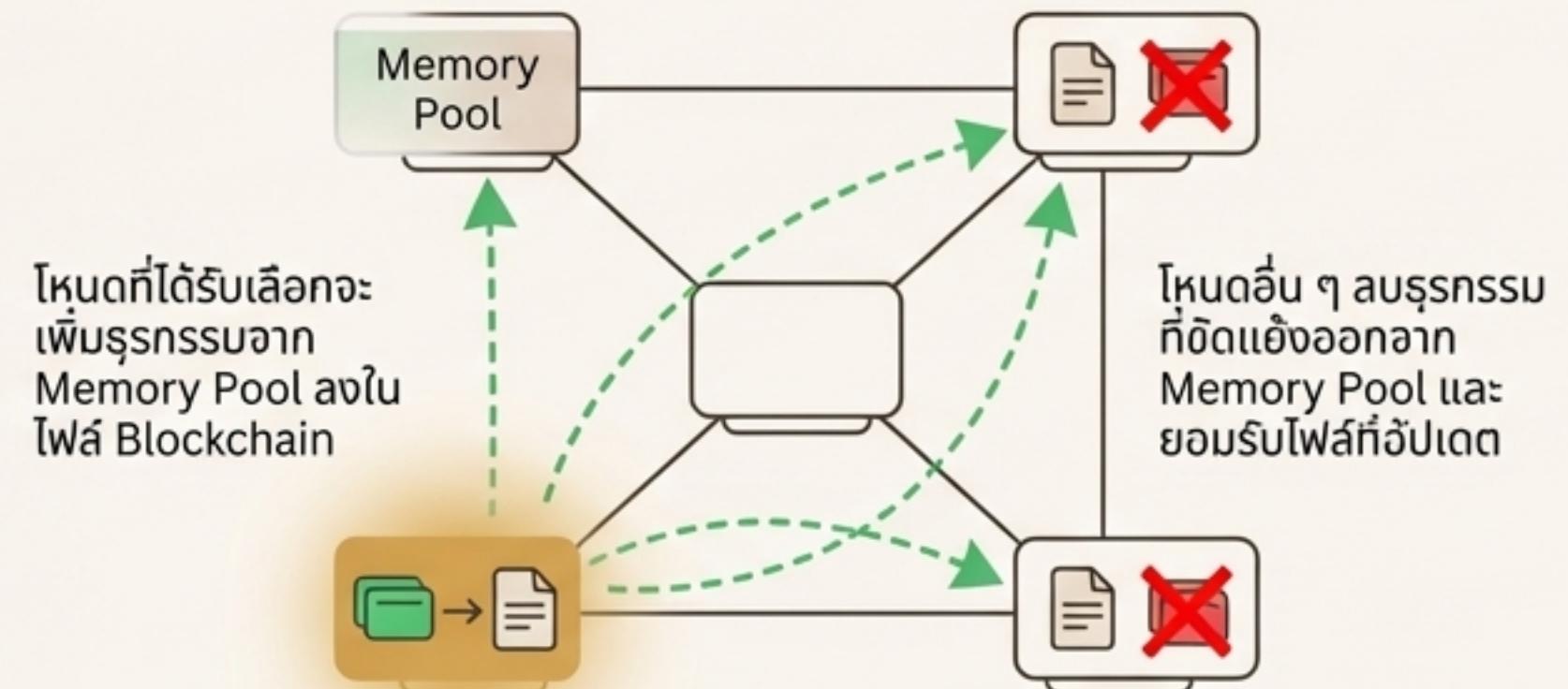
ขั้นตอนที่ 1: เก็บธุรกรรมไว้ในหน่วยความจำชั่วคราว

ขั้นตอนที่ 1: เก็บธุรกรรมไว้ในหน่วยความจำชั่วคราว
แทนที่จะบันทึกลงไฟล์กันที ทุกโนนด (คอมพิวเตอร์) ในเครือข่าย จะเก็บธุรกรรมที่ได้รับมาใหม่ไว้ในพื้นที่ที่เรียกว่า 'Memory Pool' ก่อน



ขั้นตอนที่ 2: ตัดสินธุรกรรมที่ถูกต้องเป็นรอบ ๆ

ขั้นตอนที่ 2: ตัดสินธุรกรรมที่ถูกต้องเป็นรอบ ๆ ทุก ๆ 10 นาที จะมีโนนดหนึ่งเครื่องที่ถูกสุ่มเลือกเพื่อทำหน้าที่ รวบรวมธุรกรรมจาก Memory Pool ของตนเอง และบันทึกลงในไฟล์ Blockchain และกระจายไฟล์ที่อัปเดตแล้วไปยังโนนดอื่น ๆ กันหมด

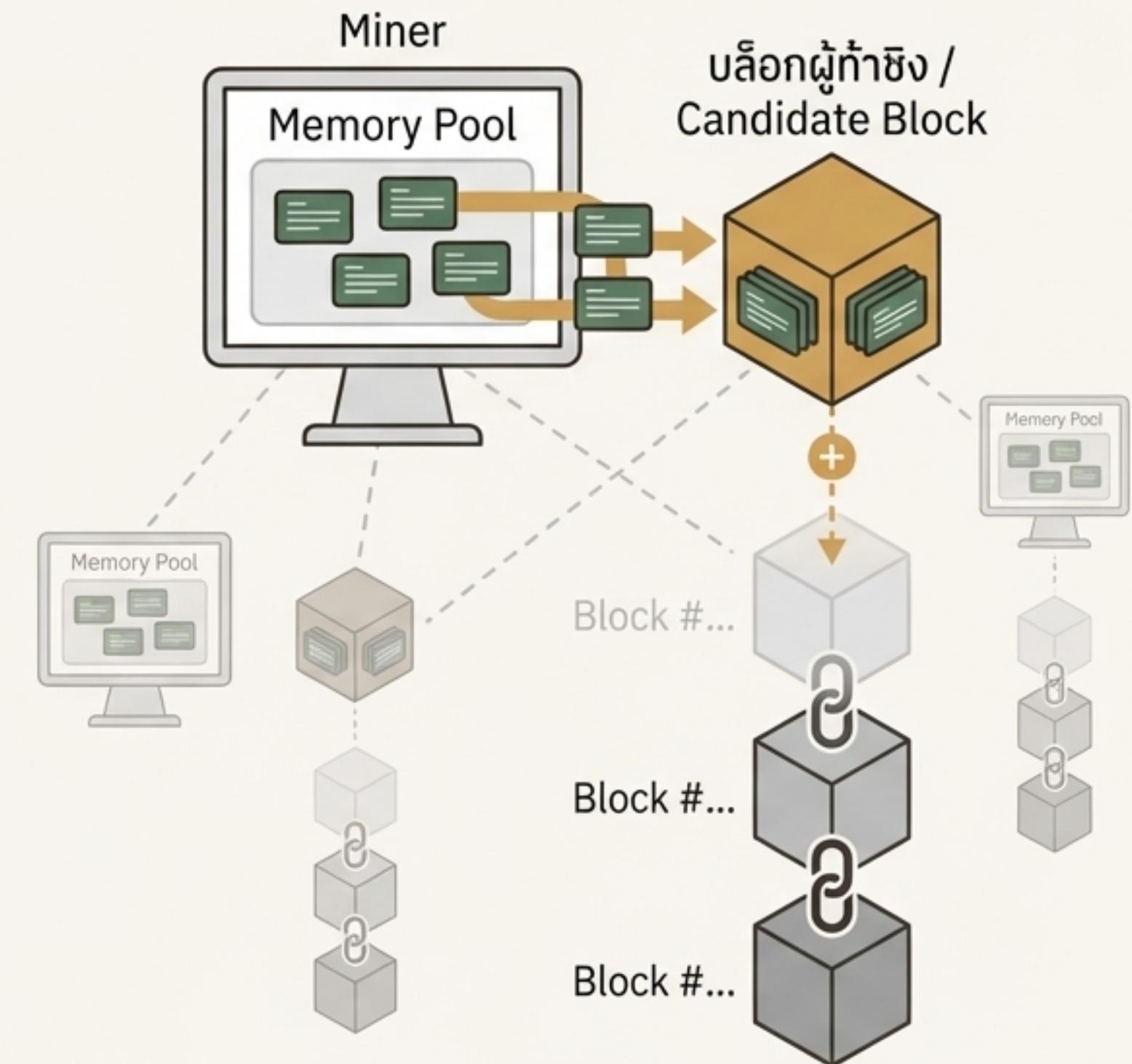


กระบวนการตัดสินใจคือการแบ่งขันกันทั่วทั้งเครือข่ายที่เรียกว่า ‘Mining’

Mining คือกระบวนการเพิ่ม ‘บล็อก’ (กลุ่มของธุรกรรม) ใหม่เข้าไปใน Blockchain

โดยนัดหมาย ก็สามารถเข้าร่วมการแบ่งขันนี้ได้ โดยรวมธุรกรรมจาก Memory Pool มาสร้าง เป็น ‘บล็อกผู้ท้าชิง’ (Candidate Block)

เป้าหมายคือการเป็นคนแรกที่สามารถเพิ่มบล็อก ของตัวเองเข้าไปต่อท้าย Blockchain ได้สำเร็จ



กลไกของ Mining: การแข่งขันแก้ปริศนาด้วยพลังการประมวลผล

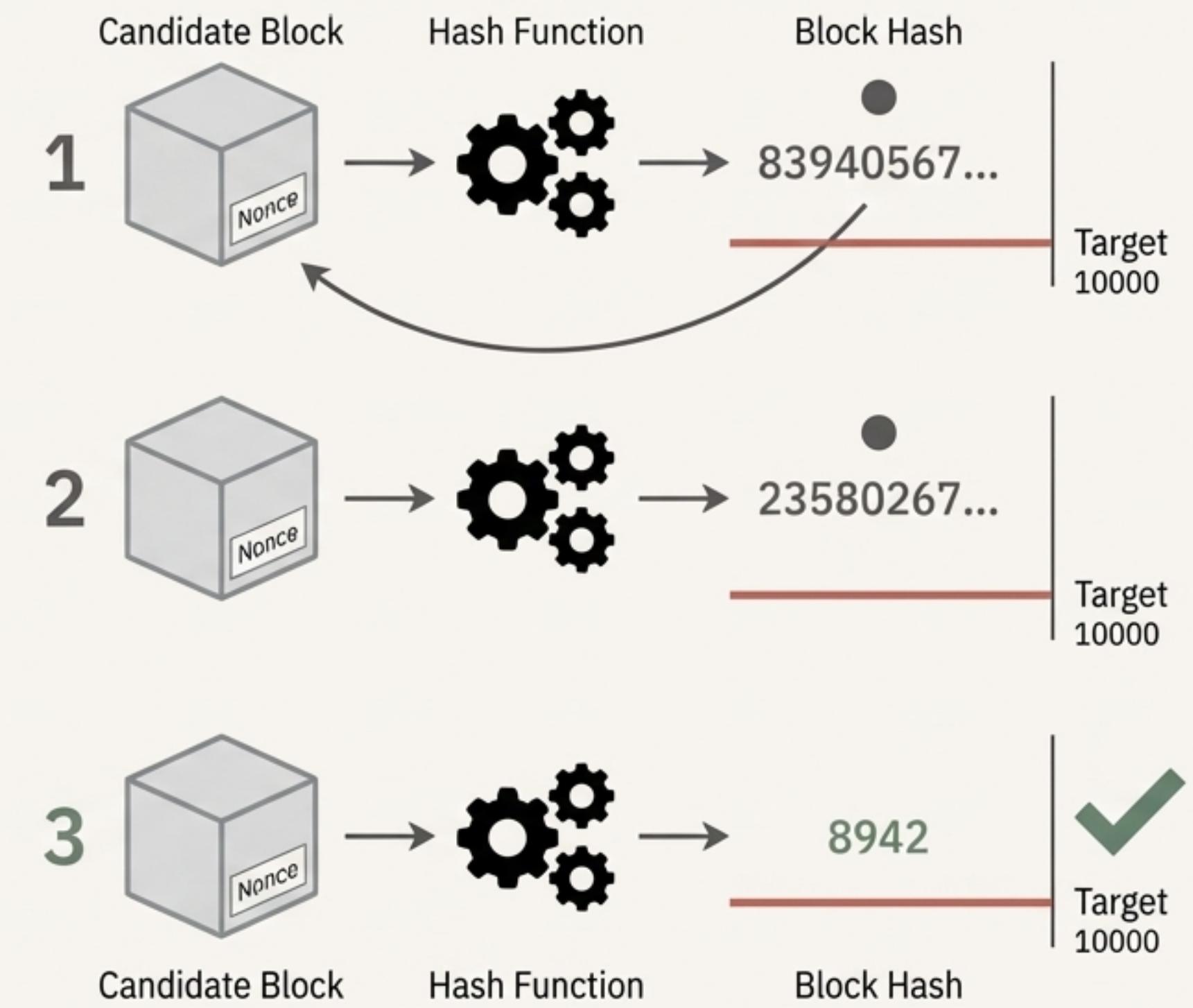
ในการเพิ่มบล็อกเข้า Blockchain โหนด (หรือ ‘Miner’) จะต้องนำข้อมูลในบล็อกไปผ่าน Hash Function

Hash Function จะเปลี่ยนข้อมูลให้เป็นตัวเลขสุ่มที่ไม่สามารถคาดเดาได้ เรียกว่า Block Hash

กฎикаคือ: Block Hash ที่ได้ จะต้องมีค่าน้อยกว่า หรือเท่ากับค่า Target ที่เครือข่ายกำหนดไว้

Miner จะต้องปรับค่าข้อมูลในบล็อกเล็กน้อย (เรียกว่า Nonce) และนำไป Hash ซ้ำ ๆ ไปเรื่อย ๆ จนกว่าจะได้ Block Hash ที่ตรงตามเงื่อนไข

นี่คือการแข่งขันที่ใช้พลังประมวลผล ใครหาเจอก่อนคือผู้ชนะ

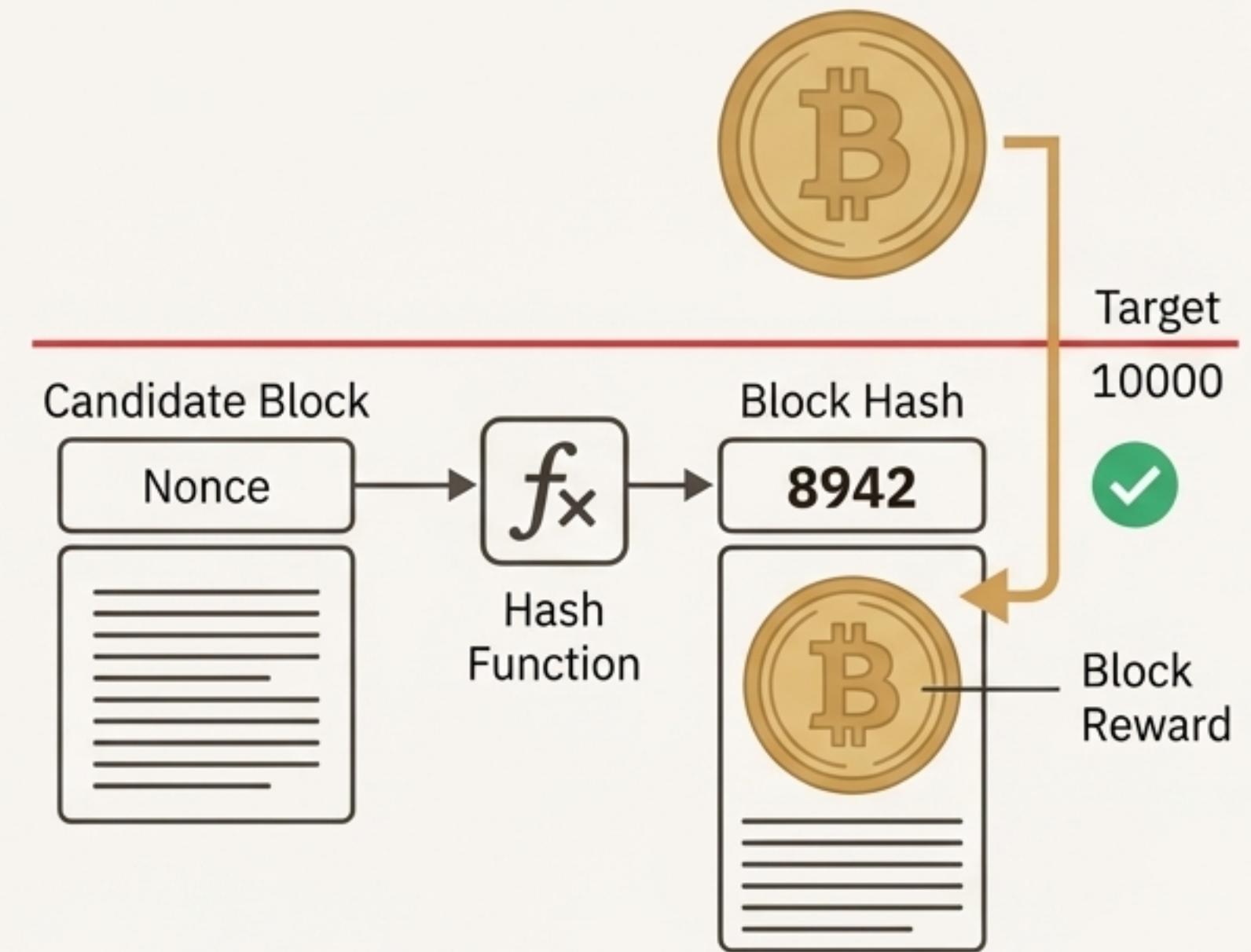


แล้ว Bitcoin ใหม่มาจากไหน? นี่คือรางวัลสำหรับผู้ช่วยการ Mining

เพื่อเป็นแรงจูงใจให้ผู้คนใช้พลังประมวลผลในการรักษาความปลอดภัยของเครือข่าย ทุกครั้งที่มีการสร้างบล็อกใหม่สำเร็จ ระบบจะสร้าง Bitcoin จำนวนหนึ่งขึ้นมาซึ่งไม่เคยมีอยู่มาก่อน

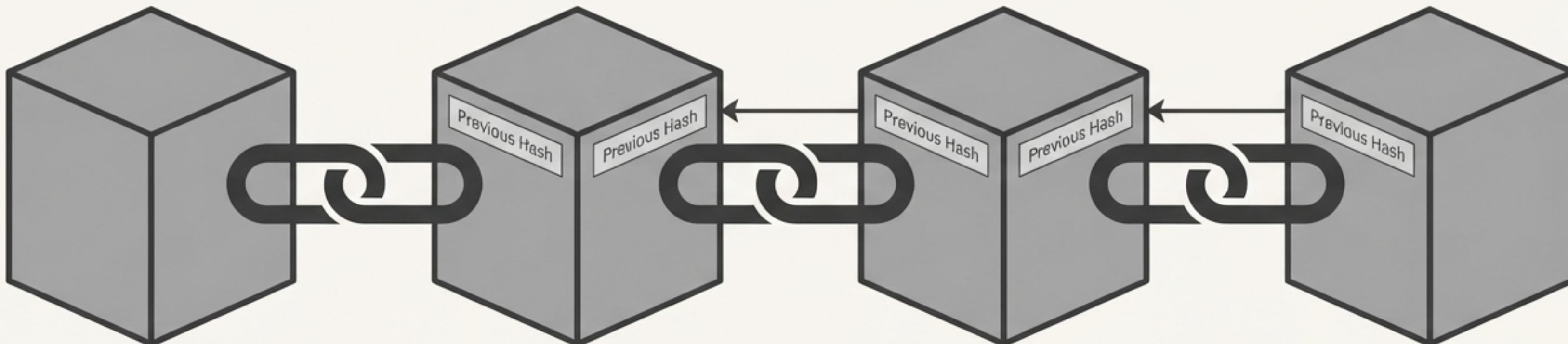
Miner ที่ชนะการแข่งขัน (ผู้ที่หา Block Hash ที่ถูกต้องได้เป็นคนแรก) จะได้รับ Bitcoin ใหม่เหล่านี้เป็นรางวัล เรียกว่า Block Reward

นี่คือเหตุผลที่กระบวนการนี้ถูกเรียกว่า ‘การขุด’ (Mining)



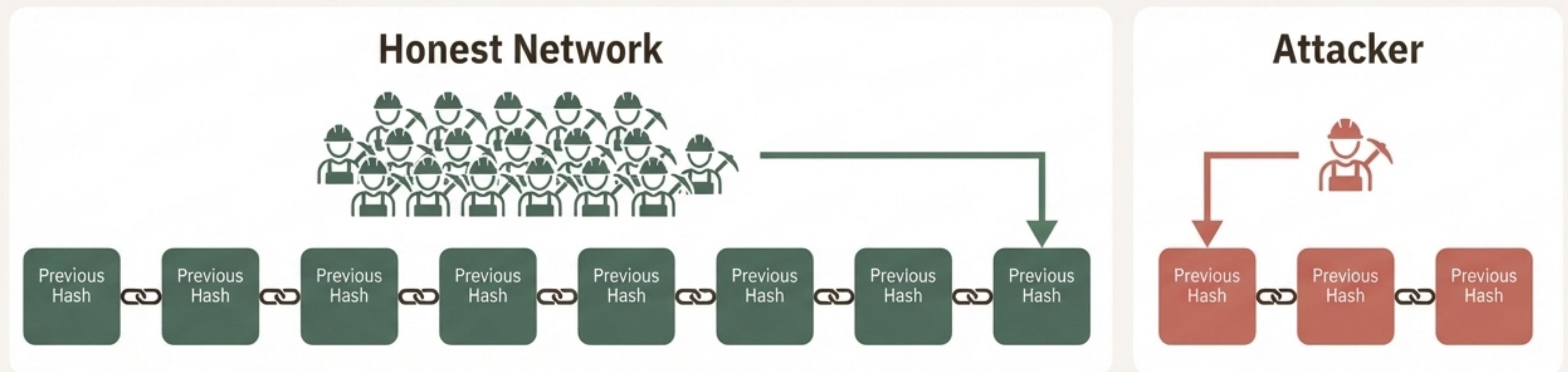
ผลลัพธ์คือ ‘Blockchain’: ໂນ່ຍບ້ອງບັນທຶກທີ່ເຊື່ອມຕ່ອກັນເປັນ ປະວັດສາສຕຣ໌ທີ່ແປລ່ຽນແປລ່ອງໄມ່ໄດ້

- ຮຸຮກຮ່າມໄມ່ໄດ້ຄູກບັນທຶກທີ່ລະຮາຍການ ແຕ່ຈະຄູກຮວມກັນເປັນ “ບັນທຶກ”
- ແຕ່ລະບັນທຶກໃໝ່ກໍ່ຄູກສ້າງຂຶ້ນ ຈະມີການອ້າງອີງຄິ່ງບັນທຶກກ່ອນหน້າເສນວ ກຳໃຫ້ເກີດການເຊື່ອມຕ່ອກັນເປັນສາຍໂຈ່ (Chain)
- ກຕິກາທີ່ສໍາຄັນທີ່ສຸດຄົວ: **ເຄື່ອງຂ່າຍຈະຍອມຮັບສາຍໂນ່ຍບ້ອງບັນທຶກ (Chain)** ທີ່ຢ່າວທີ່ສຸດທີ່ສຸດ ວ່າເປັນເວຼອຮັບທີ່ຄູກຕ້ອງເສນວ



'กฎสายโซ่ที่ยาวที่สุด' ทำให้การแก้ไขประวัติศาสตร์แทบเป็นไปไม่ได้

เนื่องจากทุกคนยึดถือสายโซ่ที่ยาวที่สุดเป็นหลัก Miners จึงมีแรงจูงใจที่จะสร้างบล็อกต่อจากปลายสุดของสายโซ่ที่ยาวที่สุดเท่านั้น หากผู้ไม่หวังดีต้องการจะแก้ไขธุรกรรมในอดีต พวกเขายังต้องสร้างสายโซ่ใหม่ขึ้นมาแห่งหนึ่ง และต้องสร้างให้ 'ยาวกว่า' สายโซ่เดิม การจะกำเนิดนั้นได้ ผู้โจรต้องมีพลังประมวลผลมากกว่าพลังของคนทั้งเครือข่ายรวมกัน ซึ่งเป็นเรื่องที่ยากและมีค่าใช้จ่ายมหาศาล ดังนั้น ประวัติธุรกรรมทั้งหมดจึงได้รับการปกป้องด้วยพลังงานมวลรวมของเครือข่าย

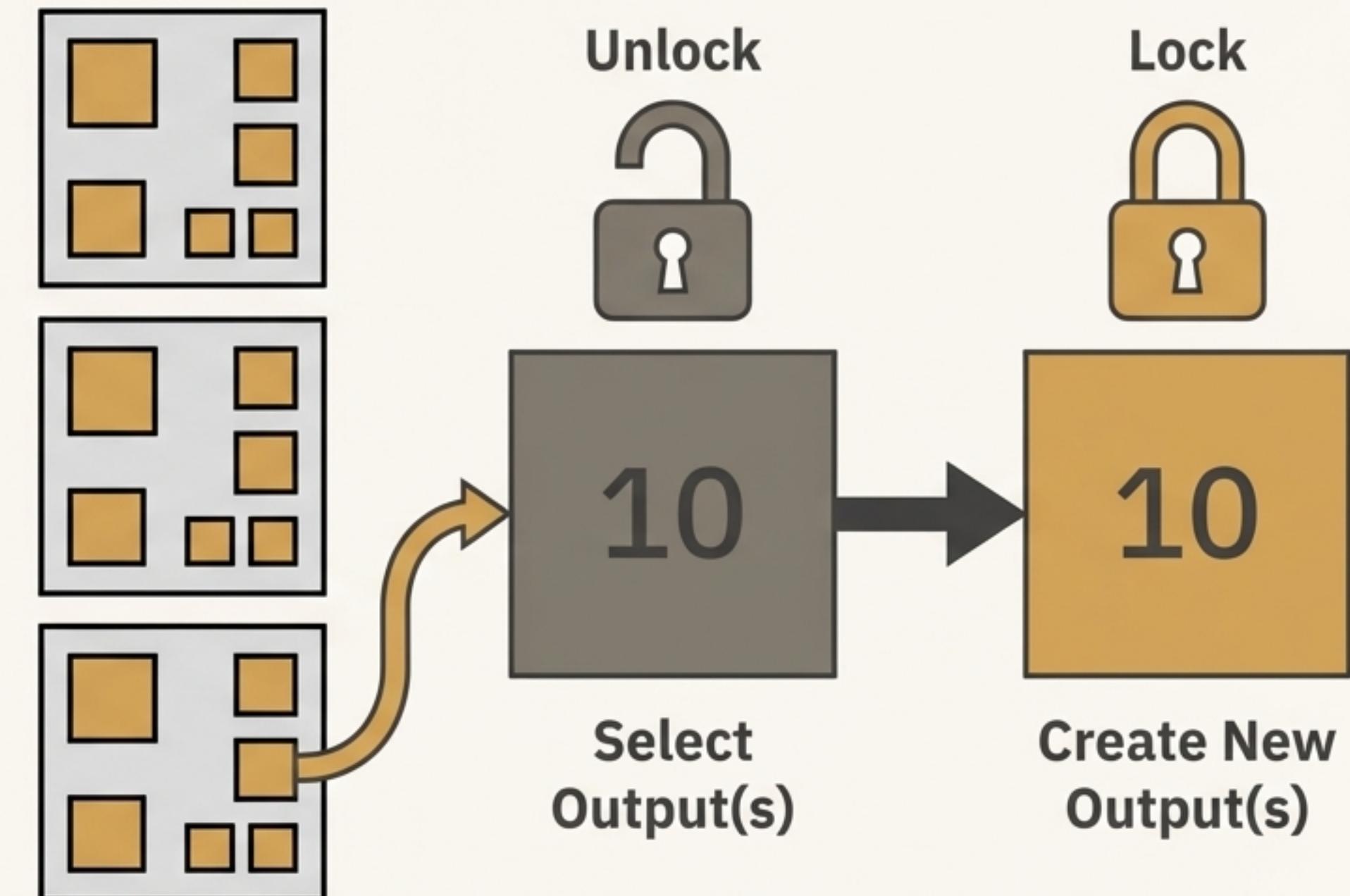


เจาะลึกธุรกรรม: Bitcoin ไม่ได้เก็บในบัญชี แต่เก็บใน ‘กล่องนิรภัยดิจิทัล’

ให้เข้าใจว่า Blockchain คือคลังเก็บ ‘กล่องนิรภัย’ (เรียกว่า **Outputs**) จำนวนมหาศาล ซึ่งแต่ละกล่องบรรจุ Bitcoin จำนวนต่าง ๆ กันไว้

เมื่อคุณ ‘ส่ง’ Bitcoin คุณไม่ได้อ่อนเงิน ออกจากบัญชี แต่คุณกำลังทำสิ่งต่อไปนี้:

1. เลือกกล่องนิรภัยที่คุณมีกุญแจไข (Unlock)
2. นำ Bitcoin ออกมา และสร้างกล่องนิรภัยใหม่ (Create New Outputs)
3. ใส่แม่กุญแจ (Lock) ที่มีเพียงผู้รับเท่านั้นที่ໄบ้ได้ลงบนกล่องใหม่



ตัวอย่าง: การส่ง Bitcoin และรับเงินก้อน

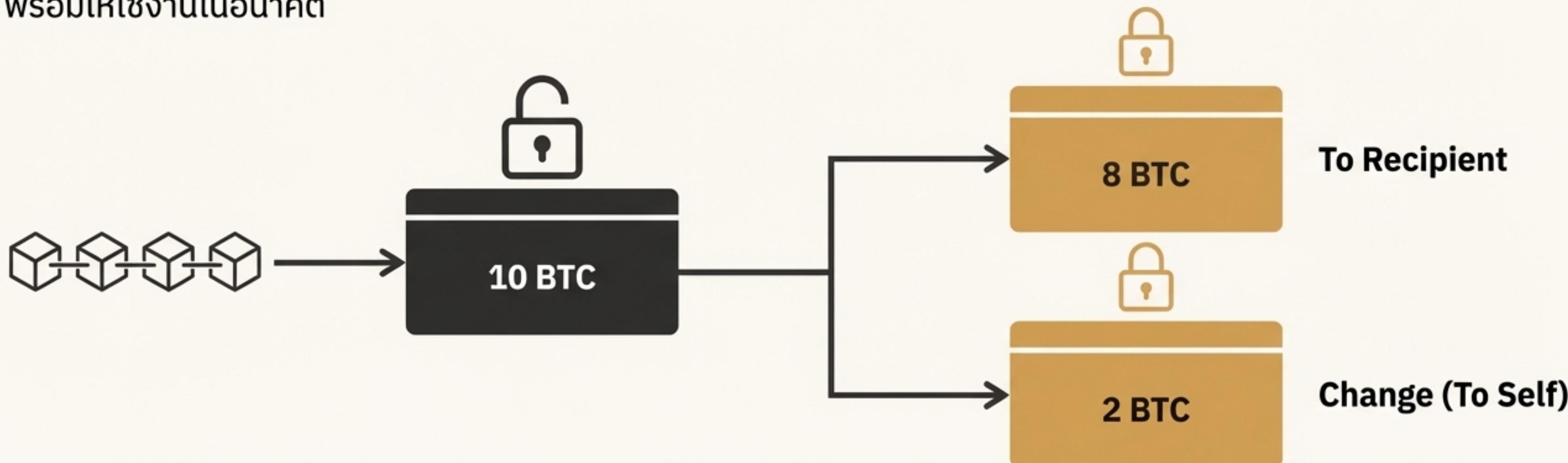
สมมติว่าคุณมีก้อนเงิน Bitcoin 10 BTC แต่ต้องการส่งให้เพื่อนแค่ 8 BTC

คุณจะปลดล็อกก้อนเงิน 10 BTC ทั้งก้อน

จากนั้นสร้าง 2 ก้อนใหม่:

- **ก้อนที่ 1:** บรรจุ 8 BTC และใส่แม่กุญแจของผู้รับ
- **ก้อนที่ 2:** บรรจุ 2 BTC และใส่แม่กุญแจของตัวคุณเองกลับเข้าไป นี่คือ "เงินก้อน"

เมื่อธุรกรรมนี้ถูกบันทึกลงใน Blockchain ก้อน 10 BTC เดิมจะถูกใช้ไป (Spent) และก้อน 8 BTC กับ 2 BTC ใหม่จะพร้อมให้ใช้งานในอนาคต



แล้วคุณ ‘เป็นเจ้าของ’ Bitcoin ได้อย่างไร? ด้วยกุญแจ 2 ดอก

Public Key (เหมือนเลขที่บัญชี)

คุณสามารถให้ Public Key ของคุณกับใครก็ได้เพื่อรับ Bitcoin...

Private Key (เหมือนรหัสผ่าน)

เป็นกุญแจลับที่คุณต้องเก็บไว้คนเดียว
ใช้สำหรับ "ไข" กล่องนิรภัยที่ถูกล็อกด้วย
Public Key ของคุณ...

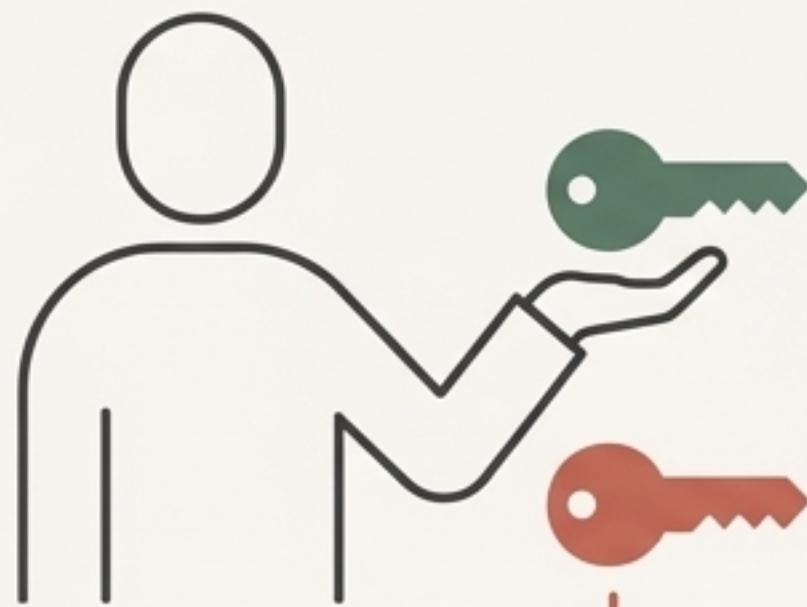


Figure A

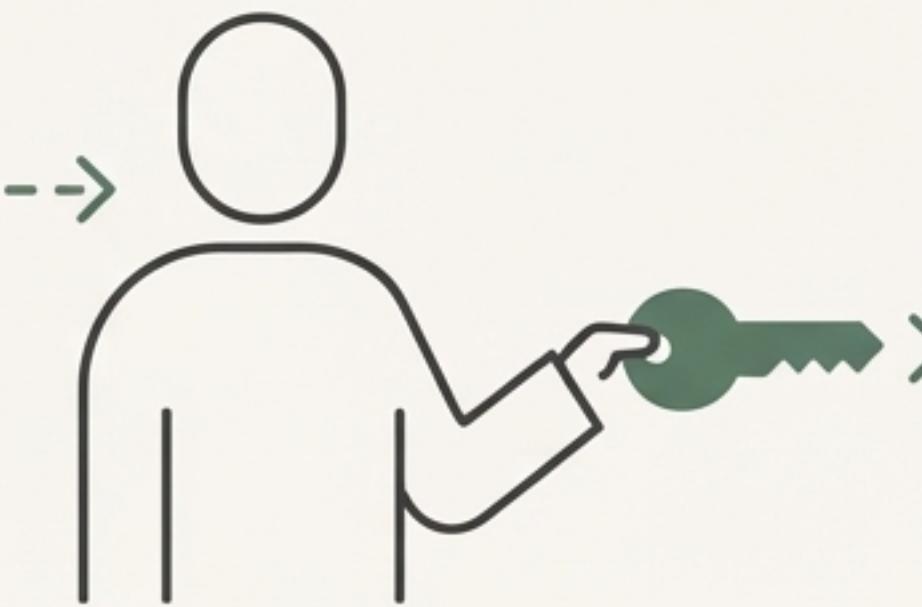


Figure B



พลังของการเข้ารหัส: กุญแจและลายเซ็นดิจิทัล

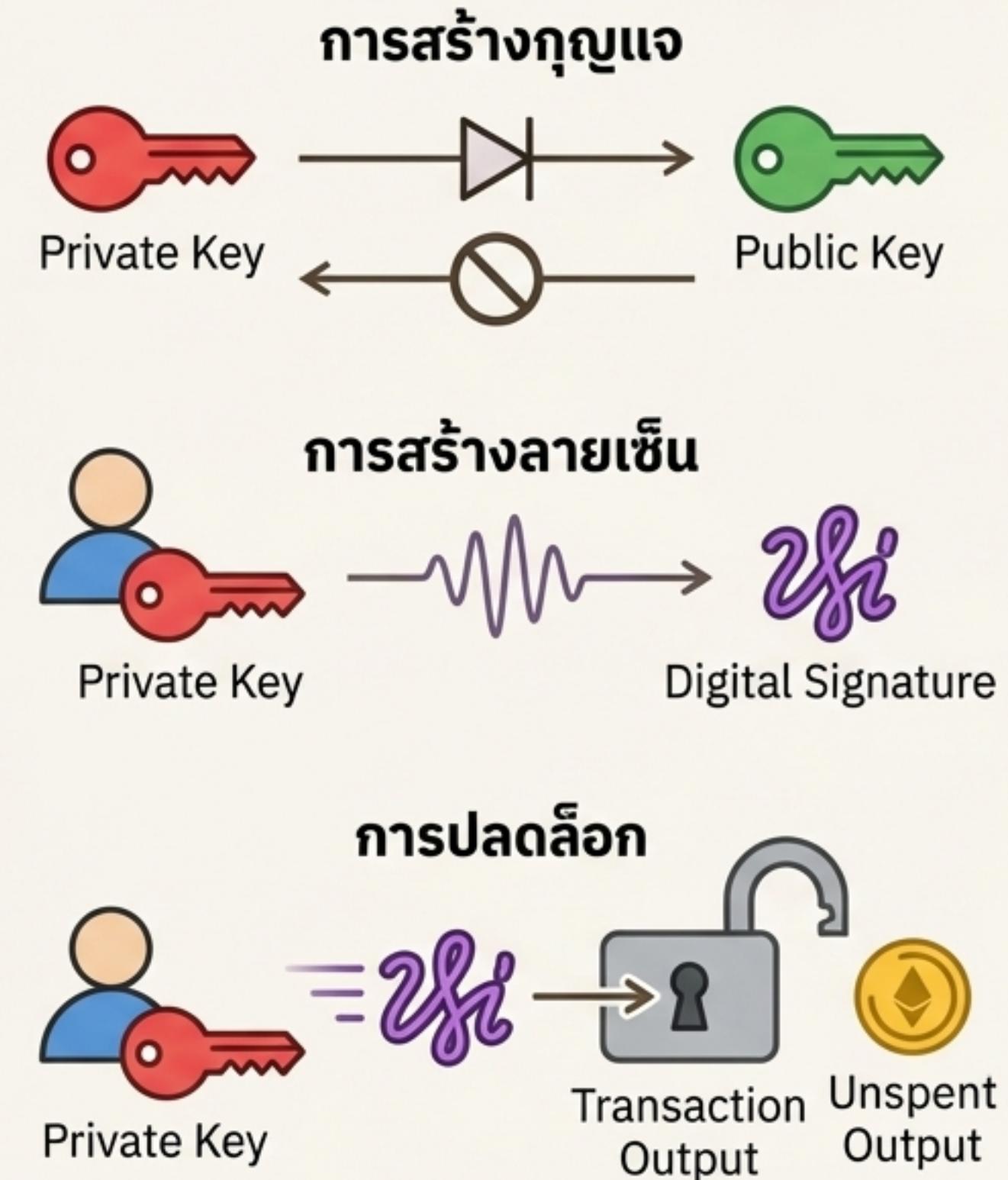
คุณสามารถสร้างกุญแจเหล่านี้ได้ด้วยตัวเองผ่าน
หลักการเข้ารหัส (Cryptography)

Private Key คือตัวเลขสุ่มขนาดใหญ่

Public Key คือตัวเลขที่คำนวณมาจาก Private
Key แต่ไม่สามารถคำนวณย้อนกลับได้

เมื่อคุณต้องการใช้จ่าย Bitcoin คุณจะใช้ Private
Key สร้าง **Digital Signature** (ลายเซ็นดิจิทัล)
สำหรับธุรกรรมนั้น ๆ

ลายเซ็นนี้ทำหน้าที่พิสูจน์ว่าคุณคือเจ้าของ Public
Key... โดยไม่ต้องเปิดเผย **Private Key** ของ
คุณ... และใช้ได้กับธุรกรรมนั้นเพียงครั้งเดียวเท่านั้น



ภาพรวมทั้งหมด: วงจรชีวิตของหนึ่งธุรกรรม Bitcoin

