

ณ ช่วงเวลาเขียน BIP-77 ยังคงอยู่ในระหว่างการสรุป และการนำเพย์จอยน์ไปดัดแปลงใช้ ยังน้อยกว่าธุรกรรมปกติมากนัก เพียงแต่ว่า ทีมงานนักพัฒนาโปรโตคอลเพย์จอยน์ได้ลงทุนลงแรงในการพัฒนา เครื่องมือและเอกสารชี้แจงมากมาย เพื่ออำนวยความสะดวกผู้ใช้ ไม่มีช่วงเวลาดีไปกว่าตอนนี้ที่เราจะเข้าร่วมการพัฒนาต่อยอดธุรกรรมชั้น เบสเลเยอร์ของบิทคอยน์ให้ดีขึ้น

เพย์จอยน์เป็นคำตอบที่ตอบโจทย์อย่างสง่างาม สำหรับการเพิ่มสมรรถภาพเสถียรภาพ ที่รักษาสันติสุขให้กับผู้ใช้ โปรโตคอลนี้ช่วยจำกัดการใช้งานพื้นที่รายบล็อก (ตัดค่าธรรมเนียมให้กับทุกคนทั่วหล้า!) และย่อหยาบการสวดส้องจากผู้ขี้ราย ด้วยตัวช่วยล้ำหลัง แม้คนที่ไม่ใช่ธุรกรรมเพย์จอยน์ก็ยังได้รับผลประโยชน์ แต่เราต้องไม่ลืมว่าสามัคคีเราอยู่ แยกอยู่เราตาย คุณประโยชน์ที่แท้จริง มาจากการนำไปใช้ของคนโดยกว้างตามสัดส่วนของธุรกรรมสามัญ เราทุกคนรับผลคล้อยได้เมื่อธุรกรรมเพย์จอยน์ได้ความยอมรับแพร่หลาย

ขอบคุณที่ให้เวลาอ่าน! พร้อมไหมไปเรียนต่อ? หากคุณต้องการได้สำเนาฟรีฉบับนี้ และบทเรียนอื่นๆอย่าลืมไป:

<https://satsie.dev/zines>

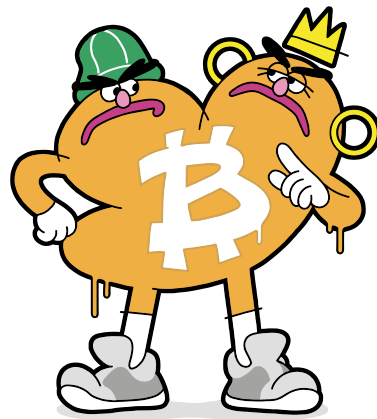
หน้า ๘ (8)

มีข้อแนะนำฉบับพิเศษสำหรับเพย์จอยน์สามข้อ

1. บีพ-79 บัสด้าเพย์ (คศ. 2018)
2. บีพ-78 เพย์จอยน์ (คศ. 2019)
3. บีพ-77 เพย์จอยน์วี2 (คศ. 2023)

ที่ผ่านมาคุณต้องเปิดเซิร์ฟเวอร์แนะนำปโหลดภัยเพื่อใช้งานเพย์จอยน์ -- สร้างอุปสรรคในการเข้าถึงอย่างมาก! BIP-77 เป็นข้อแนะนำที่เจาะจงการใช้งานง่ายกว่าที่เคยเห็นทั้งหมดในปัจจุบัน คุณแค่ใช้หน้าแอฟพลิคชั่นบนเว็บก็สามารถเชื่อมต่อ กับ **ผู้ให้บริการนามสงเคราะห์** ในฐานะบุคคลที่สาม แบบไม่ฝักใฝ่ความไว้วางใจได้ ผู้ให้บริการนามสงเคราะห์ (directory server) สามารถซัพพอร์ทคนใช้งานในมุมมองได้ และลดหย่อนความจำเป็น ของการรันเซิร์ฟเวอร์รายบุคคล สำหรับผู้ใช้ทั่วไปที่อาจขาดความรู้เชิงเทคนิค นอกจากนั้นเราสามารถเพิ่มเซิร์ฟเวอร์กลาง ระหว่างผู้ให้บริการและคนใช้ทั่วไป ด้วยพร็อกซีหลอกลืมไม่สวดส้อง เป็นตัวแทนการส่งสาร HTTP ไม่ให้ตามหาไอพีแอดเดรสของผู้ให้บริการได้ และแต่ละฝ่ายผู้ใช้บริการ ก็ยังสามารถ ใช้งานกันในรูปแบบ asynchronous ไม่พร้อมกันได้อีกด้วย (ออนไลน์กันคนละคนต่างเวลา) เพราะว่าไดเรกทอรีเซิร์ฟเวอร์สามารถรับมอบฉันทะในการส่งสาส์นระหว่างผู้ใช้ ท้ายสุดแล้ว บีพ-77 ยังรองรับการเข้ารหัสตรวจสอบสิทธิ์อีกด้วย ผู้ให้บริการจึงสามารถใช้ประโยชน์ ของแบบร่างพึงประสงค์นี้ ในการรักษาความเป็นส่วนตัวของแต่ละบุคคล ไม่บิปรัดให้ผู้โหลดหย่อนหรือละวาง ไพเรเวซีและความปลอดภัยแต่เช่นใด

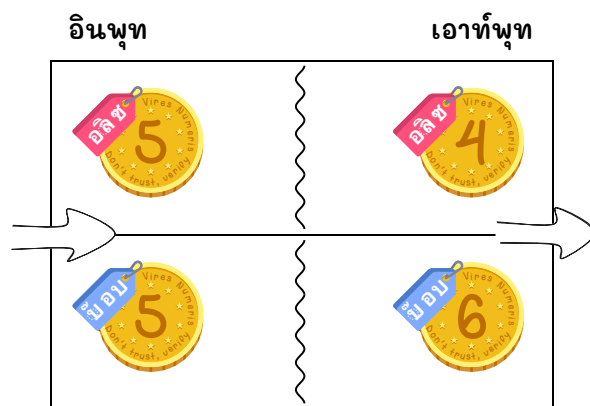
หน้า ๖ (6)



เพย์จอยน์

นิตยสารกะทัดรัดเรื่องเพย์จอยน์:
มันคืออะไร ทำไมเลิศ และทำงานอย่างไร
@satsie ☆ <https://satsie.dev/zines>
อัปเดตล่าสุด: JULY 2024

โดยการใช้เพย์จอยน์ ผู้รับเสนออินพุตร่วมสร้างธุรกรรมได้ ถ้าหากบ๊อบ มีเหรียญบิทคอยน์จำนวน 5 BTC และต้องการใช้เหรียญนี้ตอบรับ ธุรกรรมเพย์จอยน์ หน้าตาธุรกรรมจะเป็น:



กรณีที่เราเห็นนี้ดีกว่าตรงไหน? ผลประโยชน์แรกเลยก็คือ **สมรรถภาพเสถียรภาพ** โดยนิยามแล้วเพย์จอยน์ ใช้การรวมมัดธุรกรรม บนปลายทางในทั้งสองกรณี บ๊อบมี 6 BTC เท่ากัน แต่มีผลต่างเล็กน้อยในการแสดงผลลัพธ์ กรณีแรกบ๊อบได้รับเหรียญ 1 BTC จากอลิซและ ถืออีกหนึ่งเหรียญจำนวน 5 BTC อยู่แล้ว ในกรณีเพย์จอยน์บ๊อบถือหนึ่งเหรียญจำนวน 6 BTC

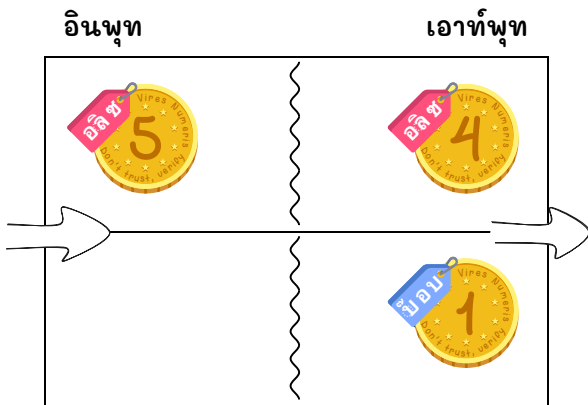
หน้า ๓ (3)

เพย์จอยน์คือวิธีการรวมมัดธุรกรรม
bitcoin แบบรักษาความเป็นส่วนตัว
และประหยัดพื้นที่บล็อก

หวนนึกว่า:

1. **bitcoin** ใช้ระบอบเอาท์พุทธุรกรรมทอน (UTXO) และ
2. เหรียญ (ข้อมูลป้อน และข้อมูลผลลัพธ์จากธุรกรรม) สามารถมีค่าเท่าไรก็ได้

สมมติว่าอลิซมีบิตคอยน์จำนวน 5 BTC ในบัญชี และสร้างธุรกรรมส่ง 1 BTC ให้กับบ๊อบ ธุรกรรมที่ถูกสร้าง (tx) จะมีหน้าตาเช่นนี้:

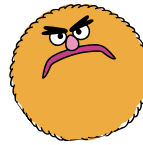


หน้า ๒ (2)

การที่จำนวนเหรียญ 1 BTC จากอลิซ ถูกรวมมัดไปกับจำนวนเหรียญแรกเริ่ม 5 BTC ของบ๊อบเป็นตัวอย่างของ **การรวมประกอบเหรียญ (coin consolidation)** ถือเหรียญมากหลายจ่ายค่าธรรมเนียมมากมันคงไม่ดีใช่มั้ย? หากเราจำกัดขึ้นเหรียญที่ถือครองให้น้อยลงได้ แทนที่การสร้างธุรกรรมโอนส่ง BTC แล้วรวมเหรียญหลายชิ้นอีกหนึ่งธุรกรรม เพย์จอยน์ทำให้เรายิ่งป็นนัลดเดียวได้สองตัว เพิ่มปริมาณงานธุรกรรมล้นหลาม! เท่านี้ยังไม่พอ หากบ๊อบอยากใช้ BTC ที่ได้รับจากอลิซ จ่ายทอดต่อให้ชาร์ลีสล่ะ? หรือเขาอยากรับเพื่อเปิดสัญญาสภาพคล่องใหม่? เราเรียกการกำหนดล่วงหน้าให้กับเอาท์พุทธุรกรรมที่กำลังได้รับแบบนี้ว่า **ธุรกรรมตัดผ่าน (tx cut-through)** เพียงเสริมการอนุมัติอินพุทและเอาท์พุทเพิ่มเติม เพย์จอยน์ทำให้เราบีบอัด เงื่อนไขภายในธุรกรรมได้ ในเมื่ออลิซกำลังส่งมอบ BTC ให้กับบ๊อบแต่แรกเริ่ม เพย์จอยน์เพียงแค่เสริมปริมาณงาน และลดหย่อนค่าธรรมเนียมให้กับผลลัพธ์เดิม เว้นธุรกรรมต่อยอดจุกจิก เรียบง่ายกว่านี้ไม่มีแล้ว ที่เราจะรวมมัดธุรกรรมระหว่างสองบุคคลได้

หน้า ๔ (4)

BIP-77 ทำงานอย่างไร



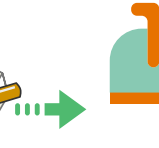
บ๊อบ: ผมอยากใช้เพย์จอยน์ เปิดอินบ็อกซ์ให้ผมได้มั๊ย ?

ผู้ให้บริการนามส่งเคราะห์: ได้เลย! นี่คือนัดเดรสของคุณครับ

บ๊อบ: คุณอลิซครับ ถ้าอยากส่ง BTC ให้ผมเมื่อไร ให้ใช้อินบ็อกซ์ตัวนี้นะครับ เราจะร่วมธุรกรรมเพย์จอยน์ไปด้วยกัน



อลิซ: โอเคค่ะ ฉันต้องการจะส่ง BTC ให้คุณบ๊อบ กำลังตั้งต้นขั้นตอนเริ่มแล้ว! ใส่กล่องจดหมายอินบ็อกซ์ของคุณ เมื่อคุณป้อนข้อมูลฝั่งรับเสร็จสิ้น ก็จะกลายเป็นธุรกรรมเพย์จอยน์



บ๊อบ: เจอแล้ว! ผมได้รับธุรกรรมเพย์จอยน์ขึ้นต้นในกล่องอินบ็อกซ์ ให้ผมป้อนข้อมูลฝ่ายรับ แล้ววางคืนลงในกล่อง

อลิซ: นี่มันตามันเช็คกล่องจดหมาย ธุรกรรมเพย์จอยน์อยู่ในนั้นด้วยข้อมูล ของสองฝ่ายเพียบพร้อม ถึงเวลาให้ฉันป่าวประกาศ บรอดแคสต์ขึ้นสู่เน็ตเวิร์กแล้ว



หน้า ๓ (7)

☆ ความเป็นส่วนตัว ☆

การสอดส่องตรวจตราบล็อกเชน มีหลักการใช้ตัวช่วยตัดสินใจ (heuristics) สำหรับการคาดคะเนลักษณะแต่ละธุรกรรม รวมไปถึงจำนวนยอดในการโอนครั้งนั้น ๆ จำนวนทอนที่ผู้ส่งได้รับคืน และเจ้าของปลายทางของเอาท์พุทแต่ละตัวหลังเกิดเหตุ ฮิวริสติกส์ที่ใช้ทั่วไป คือ การตีความว่าข้อมูลป้อนอินพุทที่มา เป็นของผู้ส่งทั้งหมด

เพย์จอยน์เป็นวิธีที่ให้ผู้ส่งและผู้รับทำงานพ้องกัน ในลักษณะที่พาฮิวริสติกส์ไขว่ไขว่ ไม่มากนักน้อยตัวสำหรับผู้สอดส่อง หลังจากทอลิซกับบ๊อบใช้เพย์จอยน์สำเร็จแล้ว การคาดคะเนว่าข้อมูลป้อนทั้งหมด มีที่มาจากบัญชีของอลิซผู้ส่ง ไม่ใช่ข้อมูลเหตุอีกต่อไป แต่ธุรกรรมดังกล่าวมีลักษณะหน้าตาเหมือนเดิม เปรียบดั่งอลิซป้อนหลายอินพุทใช้เท่านั้นเอง

สำหรับเรื่องนี้ เพย์จอยน์ส่งเสริมความเป็นส่วนตัว ของธุรกรรมรายบล็อกในทันที ตั้งแต่การจ่ายเป็นต้น

หน้า ๕ (5)