

At the time of writing, BIP-77 is still being finalized, and payjoin adoption is relatively low. However the payjoin team has been hard at work on impressive new tools and docs. There's no time like the present to implement it and improve base layer tx!

Payjoin is an elegant solution for increasing scalability and preserving privacy. It saves block space (lower fees for all!) and weaken blockchain surveillance heuristics. Even those that don't use it benefit, but it's a team effort! The advantages are proportional to the level of adoption. Everyone stands to gain from widespread payjoin use.

Thanks for reading! Ready to learn more? Want free copies of this and other zines? Visit:

<https://satsie.dev/zines>

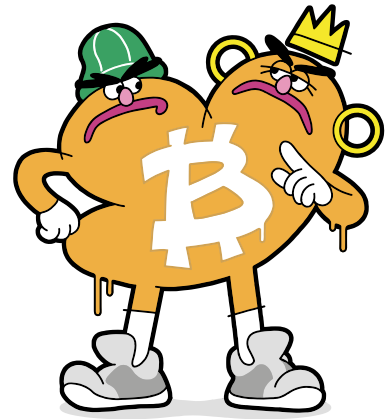
มีข้อแนะนำฉบับนี้สำหรับเพย์จอยน์สามข้อ

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

ที่ผ่านมาคุณต้องเปิดเซิร์ฟเวอร์แนะนำปโหลดภัยเพื่อใช้งานเพย์จอยน์ -- สร้างอุปสรรคในการเข้าถึงอย่างมาก! BIP-77 เป็นข้อแนะนำที่เจาะจงการใช้งานง่ายกว่าที่เคยเห็นทั้งหมดในปัจจุบัน คุณแค่ใช้หน้าแอฟพลีเคชันบนเว็บก็สามารถเชื่อมต่อ กับ **ผู้ให้บริการนามสงเคราะห์** ในฐานะบุคคลที่สาม แบบไม่ฝักใฝ่ความไว้วางใจได้ ผู้ให้บริการนามสงเคราะห์ (directory server) สามารถชี้พอร์ทคนใช้งานในมุมมองได้ และลดหย่อนความจำเป็น ของการรันเซิร์ฟเวอร์รายบุคคล สำหรับผู้ใช้ทั่วไปที่อาจขาดความรู้เชิงเทคนิค นอกจากนั้นเราสามารถเพิ่มเซิร์ฟเวอร์กลาง ระหว่างผู้ใช้บริการและคนใช้ทั่วไป ด้วยฟรีโอกี่หล่งลิมไม่ส่ดล่อง เป็นตัวแทนการส่งสาร HTTP ไม่ให้ตามหาไอพีแอดเดรสของผู้ให้บริการได้ และแต่ละฝ่ายผู้ใช้บริการ ก็ยังสามารถ ใช้งานกันในรูปแบบ asynchronous ไม่พร้อมกันได้อีกด้วย (ออนไลน์กันต่างคนต่างเวลา) เพราะว่าไดเรกทอรีเซิร์ฟเวอร์สามารถรับมอบฉันทะในการส่งสารระหว่างผู้ใช้ ท้ายสุดแล้ว บีพ-77 ยังรองรับการเข้ารหัสตรวจสอบสิทธิ์อีกด้วย ผู้ให้บริการจึงสามารถใช้ประโยชน์ ของแบบร่างพึงประสงค์นี้ ในการรักษาความเป็นส่วนตัวของแต่ละบุคคล ไม่บับรัดให้ผู้ใช้ลดหย่อนหรือละวาง โพรเวซีและความปลอดภัยแต่เช่นใด

ฟ็อกเก็ต ไทด์ ของแซตซี

ลำหรีบ



เพย์จอยน์

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

โดยการใช้เพย์จอยน์ ผู้รับเสนออินพุตร่วมสร้างธุรกรรมได้ ถ้าหากบ๊อบ มีเหรียญบิทคอยน์จำนวน 5 BTC และต้องการใช้เหรียญนี้ตอบรับ ธุรกรรมเพย์จอยน์ หน้าตาธุรกรรมจะเป็น:



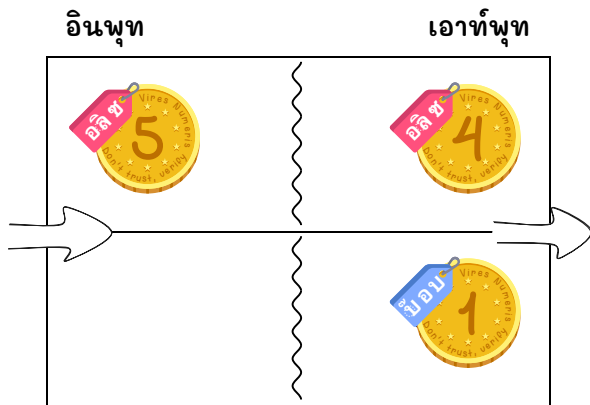
กรณีที่เราเห็นนี้ดีกว่าตรงไหน? ผลประโยชน์แรกเลยก็คือ **สมรรถภาพเสถียร** โดยนิยามแล้วเพย์จอยน์ ใช้การรวมมัดธุรกรรม บนปลายทางในทั้งสองกรณี บ๊อบมี 6 BTC เท่ากัน แต่มีผลต่างเล็กน้อยในการแสดงผลลัพธ์ กรณีแรกบ๊อบได้รับเหรียญ 1 BTC จากอลิซและ ถืออีกหนึ่งเหรียญจำนวน 5 BTC อยู่แล้ว ในกรณีเพย์จอยน์บ๊อบถือหนึ่งเหรียญจำนวน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

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:

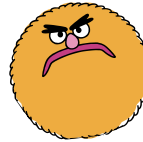


หน้า ๒ (2)

การที่จำนวนเหรียญ 1 BTC จากอลิซ ถูกรวมมัดไปกับจำนวนเหรียญแรกเริ่ม 5 BTC ของบ๊อบเป็นตัวอย่างของ **การรวมเหรียญประจบ (coin consolidation)** ถือเหรียญมากหลายจ่ายค่าธรรมเนียมมากมันคงดีไม่น้อย หากเราจำกัดขึ้นเหรียญที่ถือครองให้น้อยลงได้ แทนที่การสร้างธุรกรรมโอนส่ง BTC แล้วรวมเหรียญหลายชิ้นอีกหนึ่งธุรกรรม เพย์จอยน์ทำให้เรายิ่งประหยัดได้สองตัว เพิ่มปริมาณงานธุรกรรมล้นหลาม! เเท่านี้ยังไม่พอ หากบ๊อบอยากใช้ BTC ที่ได้รับจากอลิซ จ่ายทอดต่อให้ชาร์ลี่ล่ะ? หรือเขาอยากรับเพื่อเปิดสัญญาสภาพคล่องไลท์นิ่งใหม่? เราเรียกการกำหนดล่วงหน้าให้กับเอาท์พุทธุรกรรมที่กำลังได้รับแบบนี้ว่า **ธุรกรรมตัดผ่าน (tx cut-through)** เพียงเสริมการอนุมัติอินพุทและเอาท์พุทเพิ่มเติม เพย์จอยน์ทำให้เราบีบอัด เงื่อนไขภายในธุรกรรมได้ ในเมื่ออลิซกำลังส่งมอบ BTC ให้กับบ๊อบแต่แรกเริ่ม เพย์จอยน์เพียงแค่เสริมปริมาณงาน และลดหย่อนค่าธรรมเนียมให้กับผลลัพธ์เดิม เว้นธุรกรรมต่อยอดจุกจิก เรียบง่ายกว่านี้ไม่มีแล้ว ที่เราจะรวมมัดธุรกรรมระหว่างสองบุคคลได้

หน้า ๔ (4)

BIP-77 ทำงานอย่างไร



Bob: I want to start using payjoin. Can I have a mailbox?

Directory Server: Sure! Here's your address

Bob: Hey Alice, anytime you want to send me BTC, use my mailbox so we can make a payjoin



Alice: Ok. I want to send you BTC. I've started a transaction, and am putting it in your mailbox. Add your input and it will be a payjoin.



Bob: Look! I have a payjoin transaction in my mailbox! Let me add my input and put it back in the mailbox

Alice: My turn to check the mailbox. The payjoin transaction is in there and it's complete. Now I can broadcast it to the network!



☆ ความเป็นส่วนตัว ☆

Blockchain surveillance uses heuristics to make assumptions about the nature of a tx, including how much BTC was transferred, how much the sender got back as change, and who owns which coins. The most common heuristic for tracking users is the assumption that all inputs belong to the sender.

Payjoin lets senders and receivers work together in a way that breaks one or more of these heuristics. After Alice and Bob used payjoin, the assumption that all inputs came from Alice is no longer true. The tx looks the same as if Alice provided multiple inputs.

In this regard, payjoin instantly brings privacy to on-chain transactions, right at the moment of payment.

7

5