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:

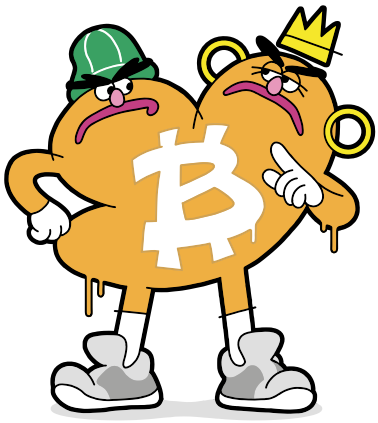
https://satsie.dev/zines

มีข้อนำเสนอบิ๊พส์สำหรับเพย์จอยน์สามข้อ

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

ที่ผ่านมาคุณต้องเปิดเซิร์ฟเว่อร์แน่นหนาปลอดภัยเพื่อใช้งานเพย์จอยน์ -- สร้างอุปสรรคในการเข้าถึงอย่างมาก! BIP-77 เป็นข้อนำเสนอที่เจาะจงการใช้งานง่ายกว่าที่เคยเห็นทั้งหมด ในปัจจุบัน คุณแค่ใช้หน้าแอพพลิเคชั่นบนเว็บก็สามารถเชื่อมต่อกับ **ผู้ให้บริการนามสงเคราะห์** ในฐานะบุคคลที่สาม แบบไม่ฝากฝังความไว้ใจได้ ผู้ให้บริการนามสงเคราะห์ (directory server) สามารถซัพพอร์ทคนใช้งานในมุมกว้างได้ และลดหย่อนความจำเป็น ของการรันเซอร์วิสรายบุคคล สำหรับผู้ใช้ทั่วไปที่อาจขาดความรู้เชิงเทคนิค นอกจากนั้นเราสามารถเพิ่มเซอร์วิสคั่นกลาง ระหว่างผู้ให้บริการและคนใช้ทั่วไป ด้วยพร็อกซี่หลงลืมไม่สอดส่อง เป็นตัวแทนการส่งสาร HTTP ไม่ให้ตามหาไอพีแอดเดรสของผู้ใช้บริการได้ และแต่ละฝ่ายผู้ใช้บริการ ก็ยังสามารถ ใช้งานกันในรูปแบบ asynchronous ไม่พร้อมกันได้อีกด้วย (ออนไลน์กันต่างคนต่างเวลา) เพราะว่าไดเร็กทอรีเซิร์ฟเวอร์สามารถรับมอบฉันทะในการส่งสาส์นระหว่างผู้ใช้ ท้ายสุดแล้ว บิ๊พ-77 ยังรองรับการเข้ารหัสตรวจสอบสิทธิ์อีกด้วย ผู้ใช้บริการจึงสามารถใช้ประโยชน์ ของแบบร่างพึงประสงค์นี้ ในการรักษาความเป็นส่วนตัวของแต่ละบุคคล ไม่บีบรัดให้ผู้ใช้ลดหย่อนหรือละวาง ไพรเวซีและความปลอดภัยแต่เช่นใด

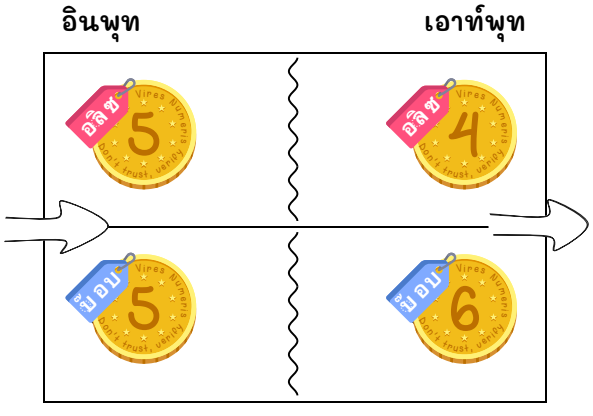
พื้นฐานเกี่ยวกับเพย์จอยน์ สำหรับ



เพย์จอยน์

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

โดยการใช้เพย์จอยน์ ผู้รับเสนออินพุทร่วมสร้างธุรกรรมได้ ถ้าหากบ๊อบ มีเหรียญบิทคอยน์จำนวน 5 BTC และต้องการใช้เหรียญนี้ตอบรับ ธุรกรรมเพย์จอยน์ หน้าตาธุรกรรมจะเป็น:



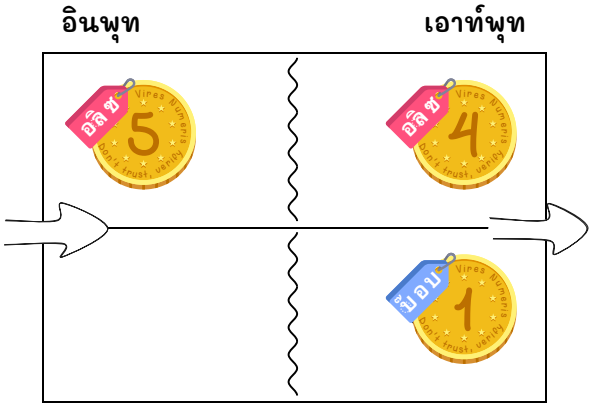
กรณีที่เห็นนี้ดีกว่าตรงไหน? ผลประโยชน์แรกเลยก็คือ **สมรรถภาพเสกลลิ่ง** โดยนิยามแล้ว เพย์จอยน์ ใช้การรวบมัดธุรกรรม บนปลายทางในทั้งสองกรณี บ๊อบมี 6 BTC เท่ากัน แต่มีผลต่างเล็กน้อยในการแสดงผลลัพธ์ กรณีแรกบ๊อบได้รับเหรียญ 1 BTC จากอลิซและ ถืออีกหนึ่งเหรียญจำนวน 5 BTC อยู่แล้ว ในกรณีเพย์จอยน์บ๊อบถือหนึ่งเหรียญจำนวน 6 BTC

เพย์จอยน์คือวิธีการรวบมัดธุรกรรม ***bitcoin*** แบบรักษาความเป็นส่วนตัว และประหยัดพื้นที่บล็อก

หวนนึกว่า:

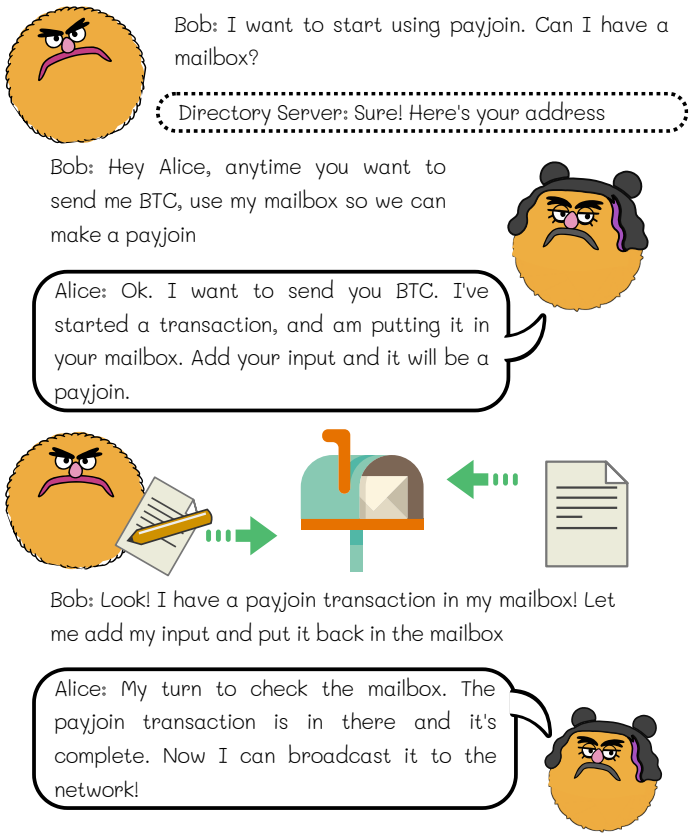
1. ***bitcoin*** ใช้ระบอบเอาท์พุทธุรกรรมทอน (UTXO) และ
2. เหรียญ (ข้อมูลป้อน และข้อมูลผลลัพธ์จากธุรกรรม) สามารถมีค่าเท่าไรก็ได้

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



การที่จำนวนเหรียญ 1 BTC จากอลิซ ถูกรวบมัดไปกับจำนวนเหรียญแรกเริ่ม 5 BTC ของบ๊อบเป็นตัวอย่างของ **การรวมประกอบเหรียญ (coin consolidation)** ถือเหรียญมากหลายจ่ายค่าธรรมเนียมมากล้น มันคงดีไม่ใช่น้อย หากเราจำกัดชิ้นเหรียญที่ถือครองให้น้อยลงได้ แทนที่การสร้างธุรกรรมโอนส่ง BTC แล้วรวมเหรียญหลายชิ้นอีกหนึ่งธุรกรรม เพย์จอยน์ทำให้เรายิงปืนนัดเดียวได้นกสองตัว เพิ่มปริมาณงานธุรกรรมล้นหลาม! เท่านี้ยังไม่พอ หากบ๊อบอยากใช้ BTC ที่ได้รับจากอลิซ จ่ายทอดต่อให้ชาร์ลีหล่ะ? หรือเขาอยากรับเพื่อเปิดสัญญาสภาพคล่องไลท์นิ่งใหม่? เราเรียกการกำหนดล่วงหน้าให้กับเอาท์พุทธุรกรรมที่กำลังได้รับแบบนี้ว่า **ธุรกรรมตัดผ่าน (tx cut-through)** เพียงเสริมการอนุมัติอินพุทและเอาท์พุทเพิ่มเติม เพย์จอยน์ทำให้เราบีบอัด เงื่อนไขภายในธุรกรรมได้ ในเมื่ออลิซกำลังส่งมอบ BTC ให้กับบ๊อบแต่แรกเริ่ม เพย์จอยน์เพียงแค่เสริมปริมาณงาน และลดหย่อนค่าธรรมเนียมให้กับผลลัพธ์มติเดิม เว้นธุรกรรมต่อยอดจุกจิก เรียบง่ายกว่านี้ไม่มีแล้ว ที่เราจะรวบมัดธุรกรรมระหว่างสองบุคคลได้

BIP-77 ทำงานอย่างไร



☆ 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.