

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>

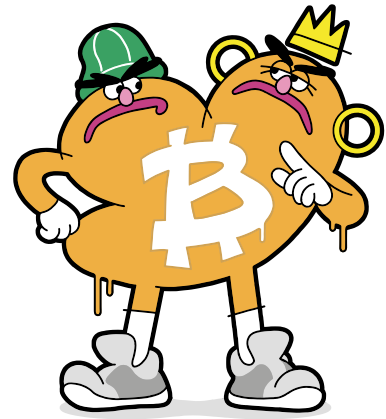
มีข้อแนะนำฉบับนี้สำหรับเพย์จอยน์สามข้อ

1. BIP-79: Bustapay (2018)
2. BIP-78: Payjoin (2019)
3. BIP-77: Payjoin V2 (2023)

BIP-77 makes using payjoin easier than ever. Previously, you had to run a secure server -- a high barrier to entry! Now, web clients are used to access untrusted, 3rd party **directory servers**. Directory servers support many users so individuals don't need to run their own. An Oblivious HTTP relay proxy server sits in front to protect user IPs. Participants can even work asynchronously (not being online at the same time) because the directory server buffers messages. BIP-77 also has authenticated encryption, allowing users to take advantage of this optimal architecture without compromising privacy or security.

พ็อกเก็ต ไทด์ ของแซตซี ดิจิทัล

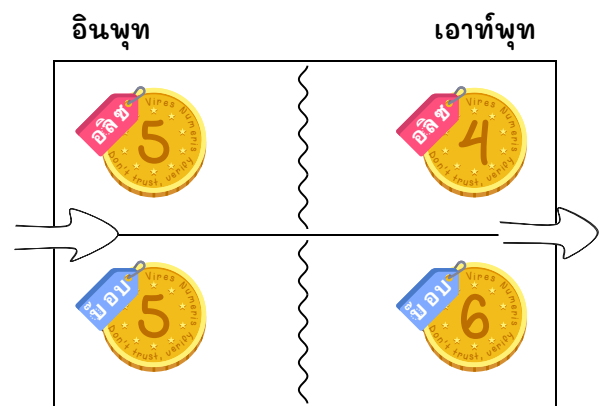
ลำหรีบ



เพย์จอยน์

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

โดยการใช้เพย์จอยน์ ผู้รับเสนออินพุตร่วมสร้างธุรกรรมได้ ถ้าหากบ๊อบ มีเหรียญบิตคอยน์จำนวน 5 BTC และต้องการใช้เหรียญนี้ตอบรับ ธุรกรรมเพย์จอยน์ หน้าตาธุรกรรมจะเป็น:



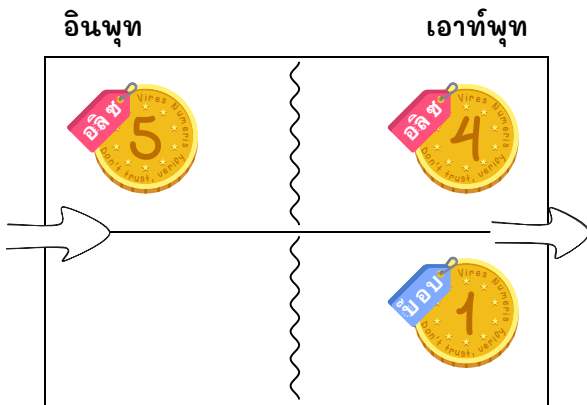
กรณีที่เราเห็นนี้ดีกว่าตรงไหน? ผลประโยชน์แรกเลยก็คือ **สมรรถภาพเสกอลิ่ง** โดยนิยามแล้วเพย์จอยน์ ใช้การรวมมัดธุรกรรม บนปลายทางในทั้งสองกรณี บ๊อบมี 6 BTC เท่ากัน แต่มีผลต่างเล็กน้อยในการแสดงผลลัพธ์ กรณีแรกบ๊อบได้รับเหรียญ 1 BTC จากอลิซและ ถืออีกเหรียญจำนวน 5 BTC อยู่แล้ว ในกรณีเพย์จอยน์บ๊อบถือหนึ่งเหรียญจำนวน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

เพย์จอยน์คือวิธีการรวมมัดธุรกรรม
bitcoin แบบรักษาความเป็นส่วนตัว
และประหยัดพื้นที่บล็อก

หวนนึกว่า:

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

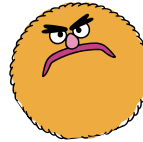
สมมติว่าอลิซมีบิตคอยน์จำนวน 5 BTC ในบัญชี และสร้างธุรกรรมส่ง 1 BTC ให้กับบ๊อบ ธุรกรรมที่ถูกสร้าง (tx) จะมีหน้าตาเช่นนี้:



หน้า ๒ (2)

The way the 1 BTC from Alice was combined with Bob's existing 5 BTC is an example of **coin consolidation**. More coins = more fees, so it's best to minimize the number of coins in your wallet. Instead of using one tx to transfer BTC, and another to consolidate coins, payjoin lets you do both at once, increasing tx throughput! That's not all. What if Bob wants to use the BTC from Alice to pay his friend Charlie? Or maybe he wants to open a Lightning channel? Using a tx for extra stuff like this is called a **tx out-through**. By allowing additional inputs and outputs, payjoin lets you pack more activity into a tx. Alice was already going to send BTC to Bob. Payjoin is just a way to raise the tx throughput and save on fees that would have gone to creating additional txs. It's the simplest way to do transaction batching between two people.

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.