Wasabi Wallet

El desafío de la privacidad: adopción y la escalabilidad

👉 Imagina un bitcoin a

$100,000 

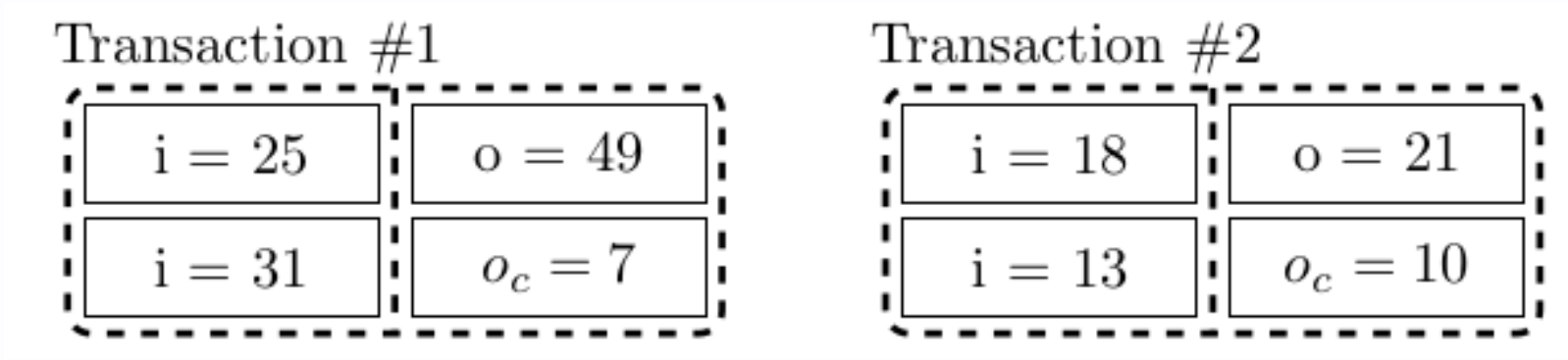
¿Cómo afectaría esto a las soluciones de privacidad?

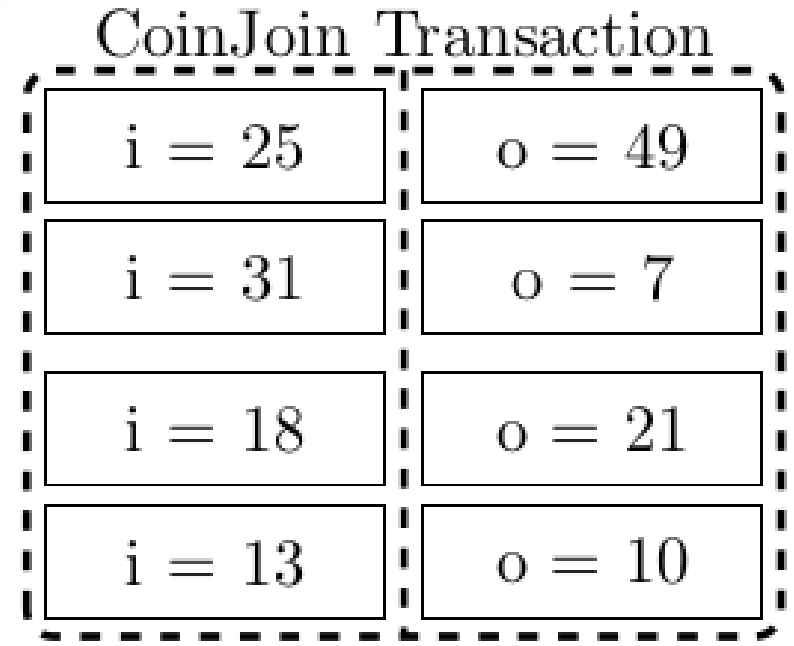
Soluciones actuales

- Coinjoin con uno mismo
- Coinjoin con quien recibe (payjoin)
- Fake coinjoins
- Coin swaps

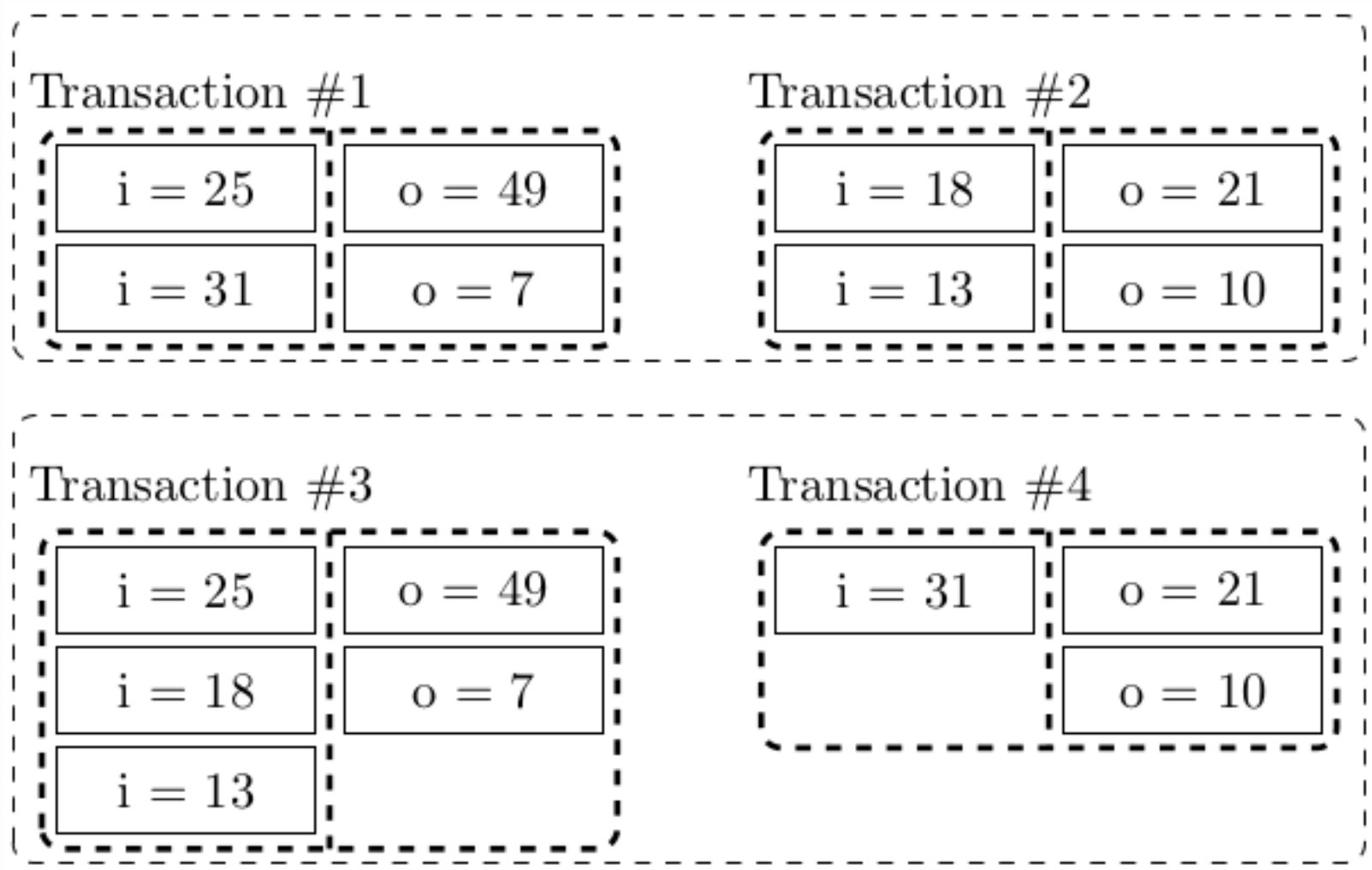
Requieren de múltiples transacciones on-chain:
Costosas

¿Qué es una tx coinjoin?





Mejora la privacidad



Knapsack (1)

- Siete participantes máximo
- Coinjoin o lote de transacciones
- Posibles subtransacciones: 32.004

$\mathrm{i} = 1.88841$	$\mathrm{o} = 1.89031$
$\mathrm{i} = 1.79381$	$\mathrm{o} = 1.81421$
$\mathrm{i} = 0.95031$	$\mathrm{o} = 0.92801$
$\mathrm{i} = 1.52261$	$\mathrm{o} = 0.66050$
$\mathrm{i} = 1.39181$	$\mathrm{o} = 0.96651$
$\mathrm{i} = 1.21961$	$\mathrm{o} = 1.11521$
$\mathrm{i} = 0.68991$	$\mathrm{o} = 1.81781$
	$\mathrm{o} = 0.26391$

Knapsack

- Transacciones válidas: 45
- Suficiente ambiguedad

Input	participation		Output	participation
1.52261	31		1.89031	31
1.21961	31		1.81421	33
1.39181	33		0.92801	33
0.68991	33		0.66050	29
1.88841	31		0.96651	31
1.79381	31		1.11521	31
0.95031	31		1.81781	31
			0.26391	31

Ejemplo: Wasabi CJ 58 inputs - 112 outputs (2)

~374144419156711147060143317175368453031918731001856 subtransacciones

Desafíos

- Eficiancia de espacio
  - Menos transacciones
  - Mayor grado de anonimato por unidad de espacio
  - Menos outputs (outputs pequeños)

Desafíos

- Eficiancia de tiempo
  - Mayor liquidez (eliminar restricciones de montos)
  - Mayor grado de ambiguedad
  - Menos outputs (menos outputs pequeños)

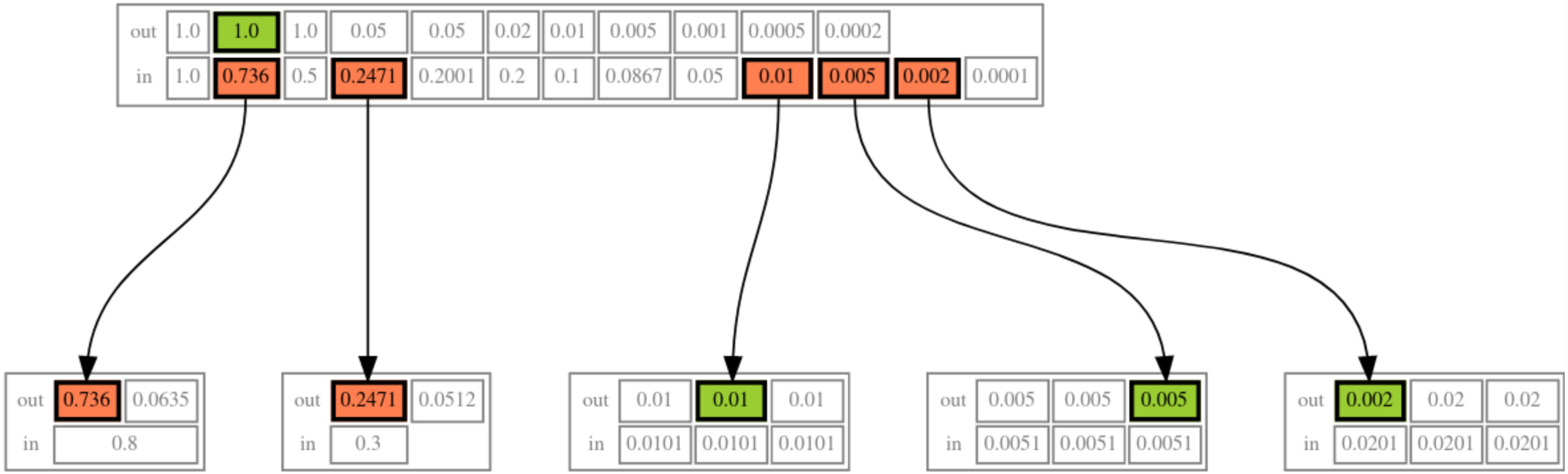
WabiSabi

Una generalización del protocolo Chaumian CoinJoin basado en un esquema keyed-verification anonymous credentials (KVAC).

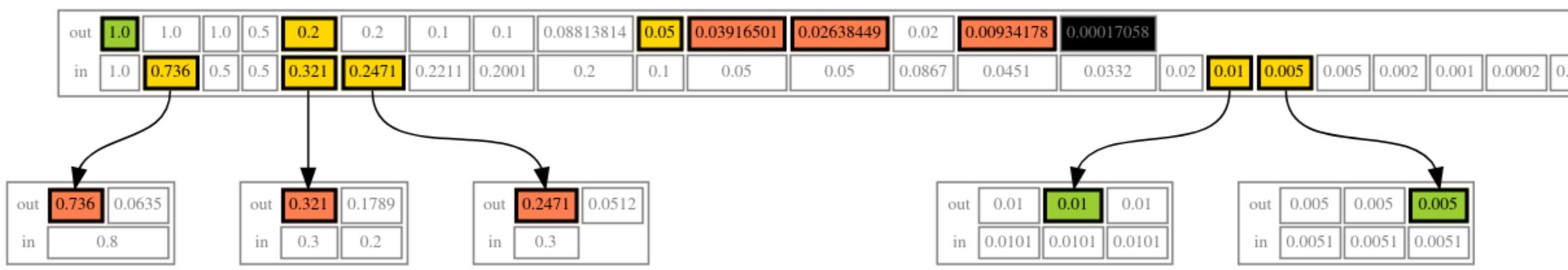
WabiSabi

- Pagos a través de coinjoins
- Pagos anónimos
- Payjoins en coinjoins

WabiSabi lotes



WabiSabi sin cambio



WabiSabi Research Club Review

1. Anonymous CoinJoin Transactions with Arbitrary Values
2. WabiSabi - A generalization of Chaumian CoinJoin based on a KVAC scheme

Lucas Ontivero (@lontivero)

https://github.com/zksnacks/walletwasabi