TABLE 1 A typology of Bitcoin transactions based on their input/output configurations and traceability of Bitcoin flows: checkmarks ✓ denote configurations such that the Bitcoin flow is traceable, while † refers to a definition introduced in the work of Chang and Svetinovic[17]

Input no	1 output	Output no 2 outputs	$n_O \geq 3$ outputs
0 input	✓ mining	✓ mining	✓ mining
1 input	1 payment or a relay	2 payments or 1 payment with change	n_O payments or $n_O - c$ payments with c changes to own wallets
	✓† (relay transaction)	✓† (peel transaction)	✓ (distribution)
$n_I \geq 2$ inputs	consolidation of fund either to own wallet or for payment	payment with or without change	multi-input multi-output
	✓ † (sweep transaction)	† (peel transaction)	(mixing/distribution)

2 | BITCOIN MIXING

A Bitcoin transaction consists of a set of inputs, and a set of outputs. Each transaction input contains a pointer to a previous transaction (output), with an associated wallet address (which will have the authority to spend the Bitcoins), while each output contains a Bitcoin amount, and the wallet address receiving the Bitcoins (more precisely, it contains a script that checks the public key and digital signature of the recipient). See the work of Narayanan et al[16] for details. The number of outputs is at least 1: It is not possible to have 0 output; however, it is possible (but not usual) to have an output with 0 amount. It is possible however to have 0 inputs, this indicates a mining operation, irrespectively of the number of outputs.

How specific Bitcoins flow from individual inputs to individual outputs within one transaction may or not be deterministically inferred, depending on the input/output configuration. In the work of Chang and Svetinovic,[17] a summary of nomenclature has been proposed for some of the configurations, which we refer to in Table 1, while specifying a typology of the transactions based on their input/output configurations