Multisignature script e acquisti online

Signature Script particolari sono utilizzati soprattutto nel caso di acquisto online, per assicurarsi di avere indietro i propri bitcoin se la merce non è spedita.

Per esempio, lo script può richiedere due chiavi private: quella del venditore e dell'acquirente. L'acquirente effettua la transazione, ma se la merce non arriva non fornirà al venditore la seconda chiave privata che quest'ultimo necessita per riutilizzare l'output come nuovo input. Insomma i bitcoin rimarrebbero bloccati nell'output senza che il venditore li possa utilizzare.

In una versione più sofisticata, detta **multisignature escrow** (acconto di garanzia a più firme), si prevede la necessità di firmare con due chiavi private su tre. Le tre parti in gioco sono il venditore, l'acquirente e una parte terza, come il sito internet su cui viene venduto il prodotto. Se c'è un contenzioso fra le due parti della transazione, il sito può fungere da arbitro e porre la sua firma. Se per esempio affiancherà la sua firma a quella dell'acquirente, sarà quest'ultimo a poter spendere l'output (da lui stesso originariamente creato con l'intento di pagare il venditore) e non il venditore. Al contrario, potrà firmare insieme al venditore permettendo a quest'ultimo di appropriarsi dell'output.

Si possono istituire metodi di multisignature vari e complessi. Venditore e acquirente possono anche accordarsi per cambiare arbitro (scegliendo un utente qualsiasi) qualora il primo arbitro scelto non fosse più ritenuto affidabile. Infatti un arbitro potrebbe rifiutarsi di mettere la firma e quindi tenere in stallo i bitcoin.