



Software ad hoc

si basava su txid



modifica scriptSig

Corsa contro il tempo

TX==FAIL => Resend!

sendrawtransaction

Possibilità di aggiungere OP\_CODE



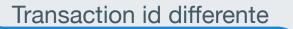
OP\_2 OP\_DROP

Modificare lo scriptSig

MT.GOX

Mt.Gox

La firma resta valida





Double spending

2 transazioni diverse, stesso utxo