Atomic Trades

Alice has ZEC.
Bob has BTC.

How can they exchange it trustlessly? and without a third party?

Basic tool – hash-time-lock-contracts (HTLCs)

1. Alice “locks” her coins in contract, publishes h(x).
2. If Bob publishes x, he can take the coins.
3. After 24 hours pass, Alice can take back the coins.

Can be implemented in bitcoin/Zcash!

Atomic Trades with HTLCs

1. Alice chooses secret x. Stores her ZEC in HTLC with h(x).
2. Bob locks his BTC in HTLC with same h(x).
3. Alice publishes x to take Bob's BTC.
4. Bob knows x now; can use it to take Alice's ZEC.

If someone aborts prematurely, the other's funds are restored after 24 hrs.