Two-Party Fair Exchange: Seller S has a digital item x. Buyer wants to exchange p coins for item x if and only if if x satisfies a condition encoded in by a predicate phi.

Fairness: Either S gets p coins and B gets item x such that phi(x) = True, or S gets no coins and B learns nothing about x.

Proven that two-party fair exchange is impossible without a trusted third party. But who can we trust?

Smart Contracts: Trusted and transparent programs executed on public networks called blockchains. Manage the transfer of cryptocurrency. Anyone can see what the smart contract sees.

FairSwap [1] replaces TTP with smart contracts. Smart Contract is an arbiter that solves disputes between S and B to ensure a fair exchange.

Circuit model of computation: If we model phi as a circuit, a cheating seller can be detected with one bad gate. B constructs a concise proof of misbehavior (POM) from the one bad gate. Smart contract can verify the POM by computing the gate themselves then settle the dispute.

Privacy Problem: Smart contract is public, leaks some of x to the world. Not suitable for confidential data.

Solution: Allow the smart contract to do the computation while hiding the values:
- Homomorphic encryption
- Circuit Randomization [2]

References: