

economics & cybercrime

cybercrime: traditional crime in technological system

can be
 vehicle to crime
 vehicle & target of crime

	provision	trade
hacking	first order (enable back) rules, exploits second order (after hack) credit card, bank info, trade secrets	online product selection, contract, delivery
non-hacking	non-traditional channels drugs, weapons, other hardware	on- and offline delivery of physical goods

a market only operates if contracts are valid/can be satisfied

principal → asks for service

agent → provides service

sustainable market equilibrium requires

best strategy { seller → deliver goods
 buyer → respect terms i.e. pay

no regulator → information asymmetry

adverse selection → buyers & seller cannot evaluate each other's characteristics

moral hazard → behavior change after contract is signed

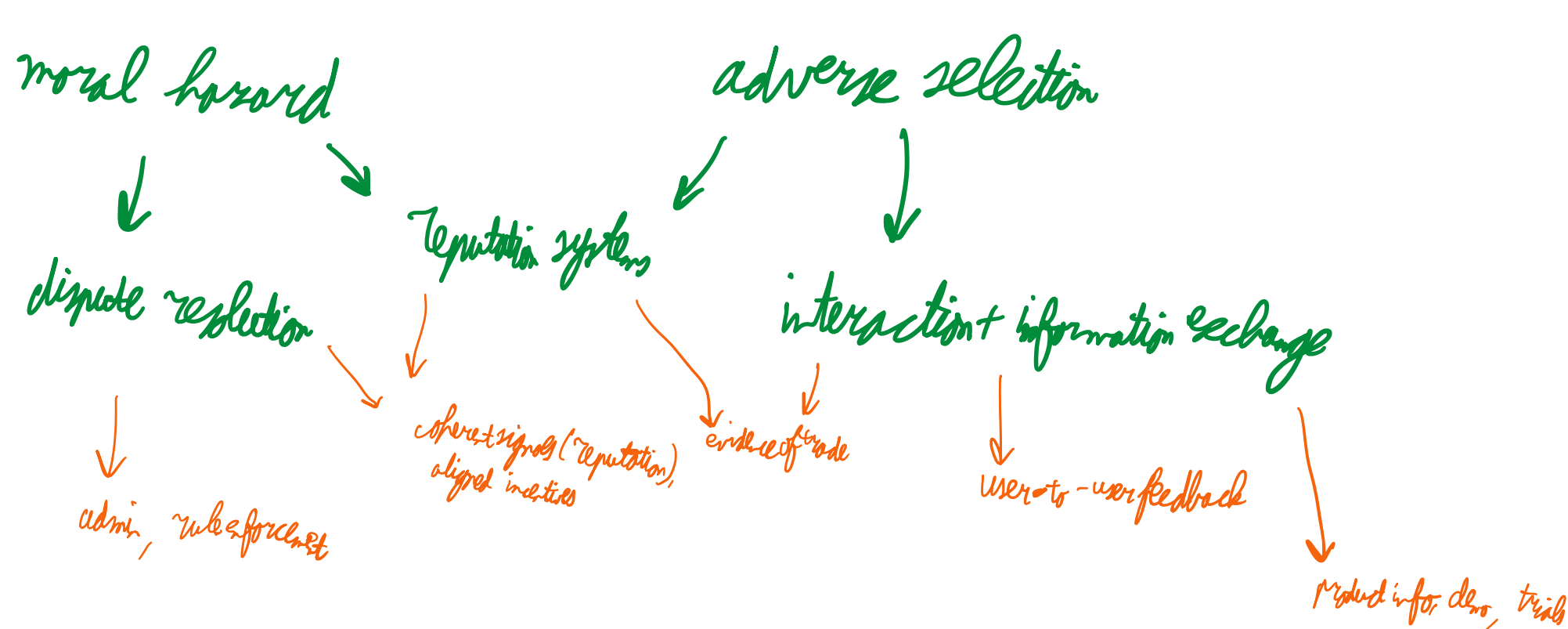
initial cybercrime markets: scam-the-scammer

interactions are criminal → contracts cannot be enforced

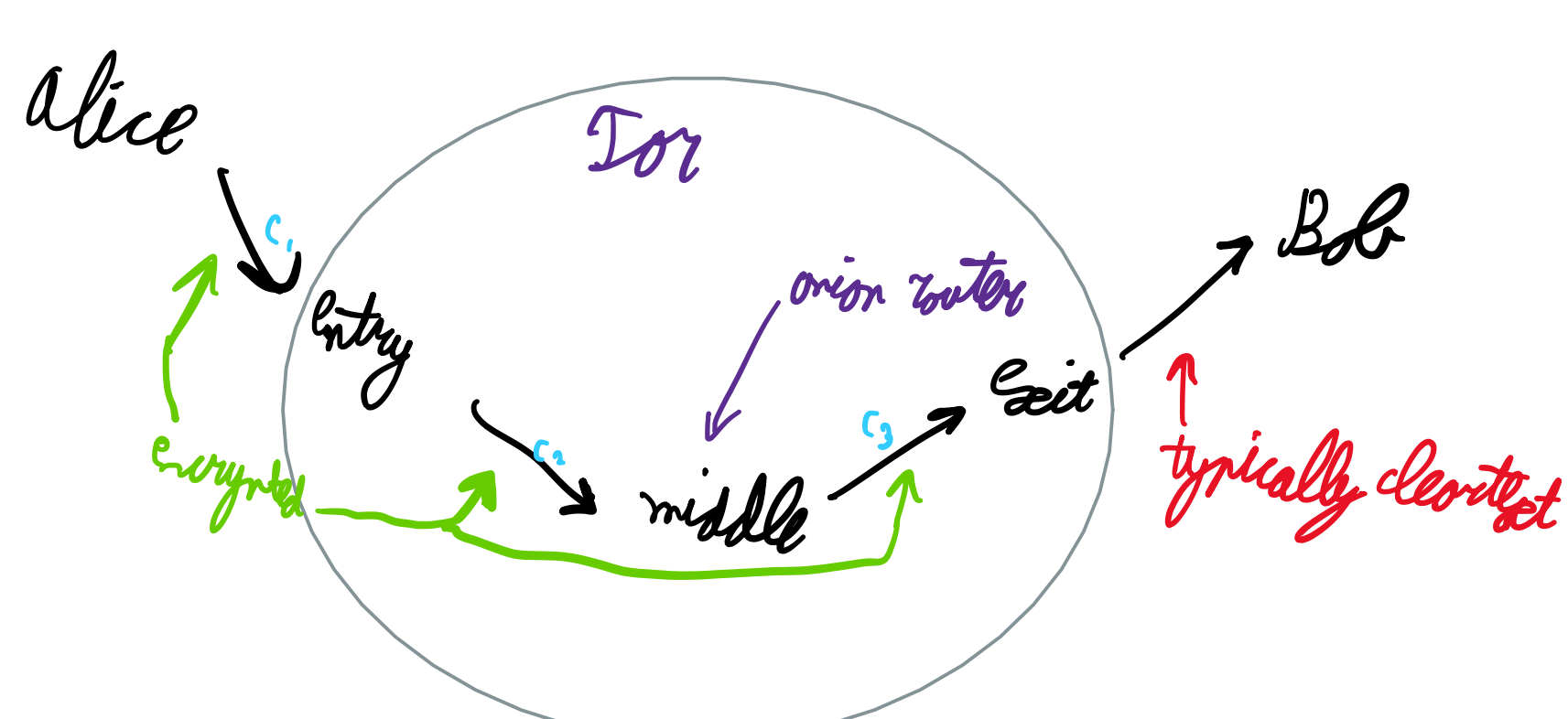
malware → forum-based markets

drugs/weapons → e-commerce

people come back to trusted vendors



Tor → onion
 both sides anonymous



Alice picks 3 random onion routers, builds Tor circuit

Onion Service

choose introduction points, build Tor circuit to them

ask introduction points to directory service

Alice request info from database

select a rendezvous point

encrypts
 writes message to Bob with one-time secret

asks introduction point to deliver it to Bob

Bob connects to rendezvous point, provides one-time secret

use Tor circuits like normal

escrow systems: money is initially received by platform; money is only released when goods are received

exit scam: platform takes money and shuts down

multi-sig escrow: two out of three parties must agree to transfer money out

largely prevents exit scam