Eclipse Attacks - Double Spending
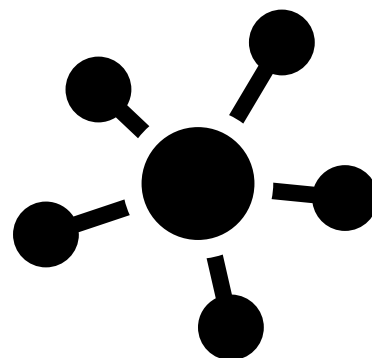
What is Double Spending?

Spending money more than once

$TX_{legitimate}$ - Pays the vendor

$TX_{doublespend}$ - Pays the adversary

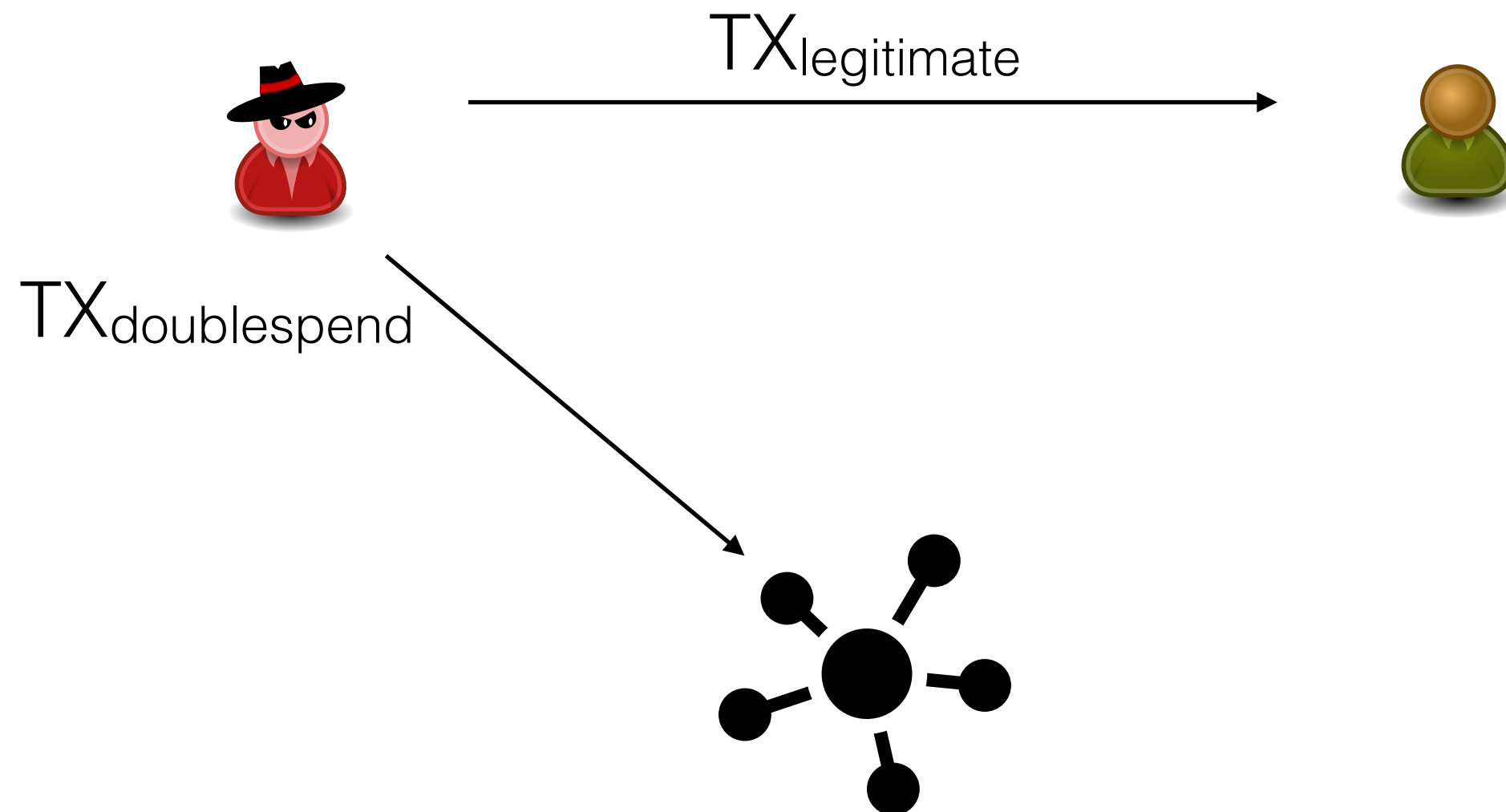# What is Double Spending?

Spending money more than once

$TX_{legitimate}$ — Pays the vendor

$TX_{doublespend}$ — Pays the adversary

$TX_{legitimate}$

$TX_{doublespend}$

What is Double Spending?

Spending money more than once

$TX_{legitimate}$ - Pays the vendor

$TX_{doublespend}$ - Pays the adversary

$TX_{legitimate}$
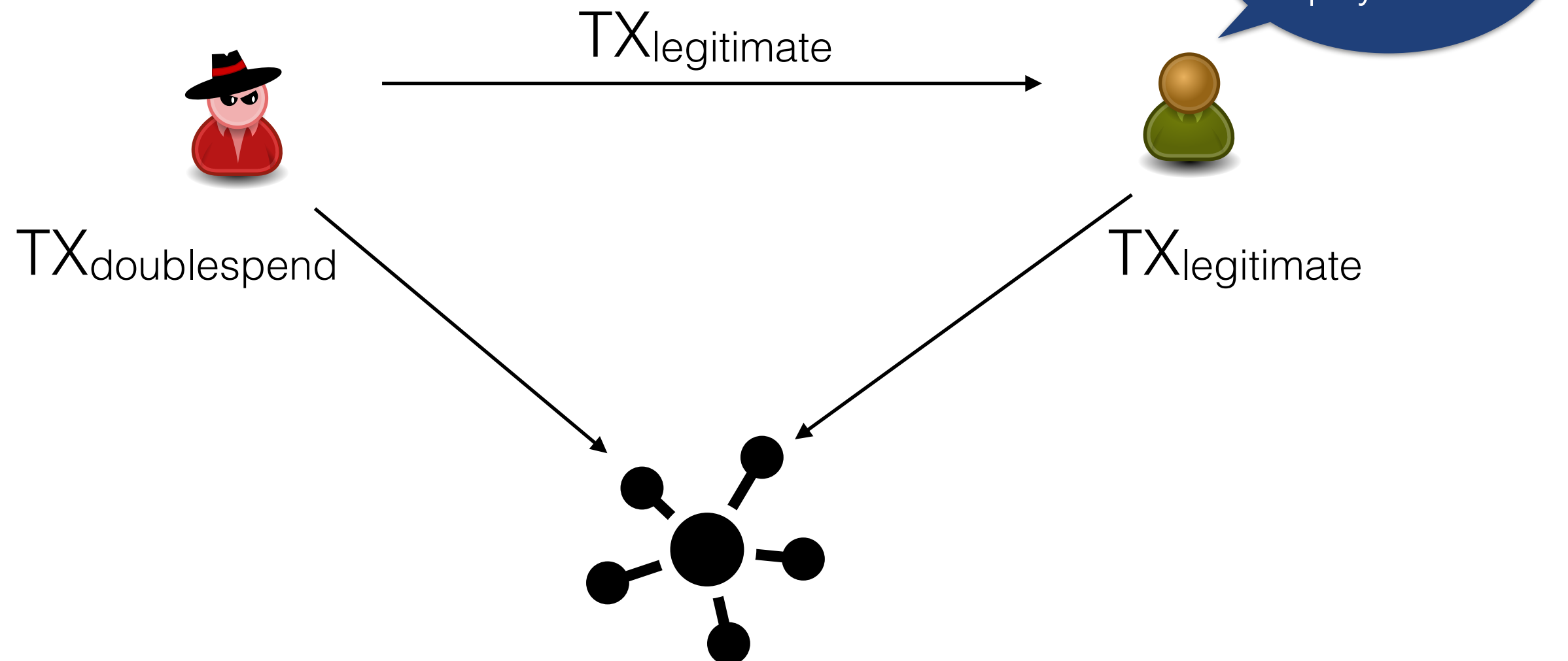
Ok, I accept the payment

$TX_{doublespend}$

$TX_{legitimate}$

What is Double Spending?

Spending money more than once

$TX_{legitimate}$ - Pays the vendor

$TX_{doublespend}$ - Pays the adversary

$TX_{legitimate}$

Goods/Service

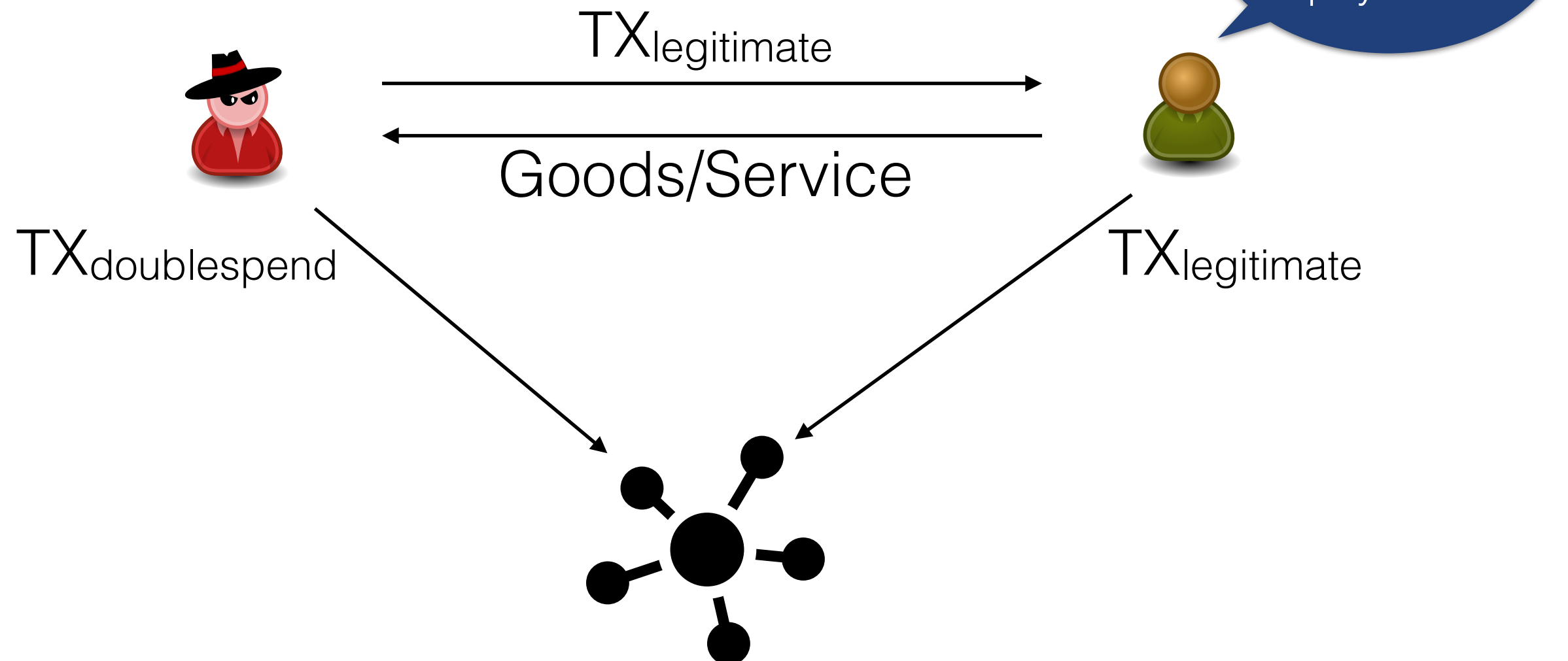Ok,
I accept the payment

$TX_{doublespend}$

$TX_{legitimate}$

What is Double Spending?

Spending money more than once

$TX_{legitimate}$ - Pays the vendor

$TX_{doublespend}$ - Pays the adversary

$TX_{legitimate}$

Goods/Service

Ok, I accept the payment

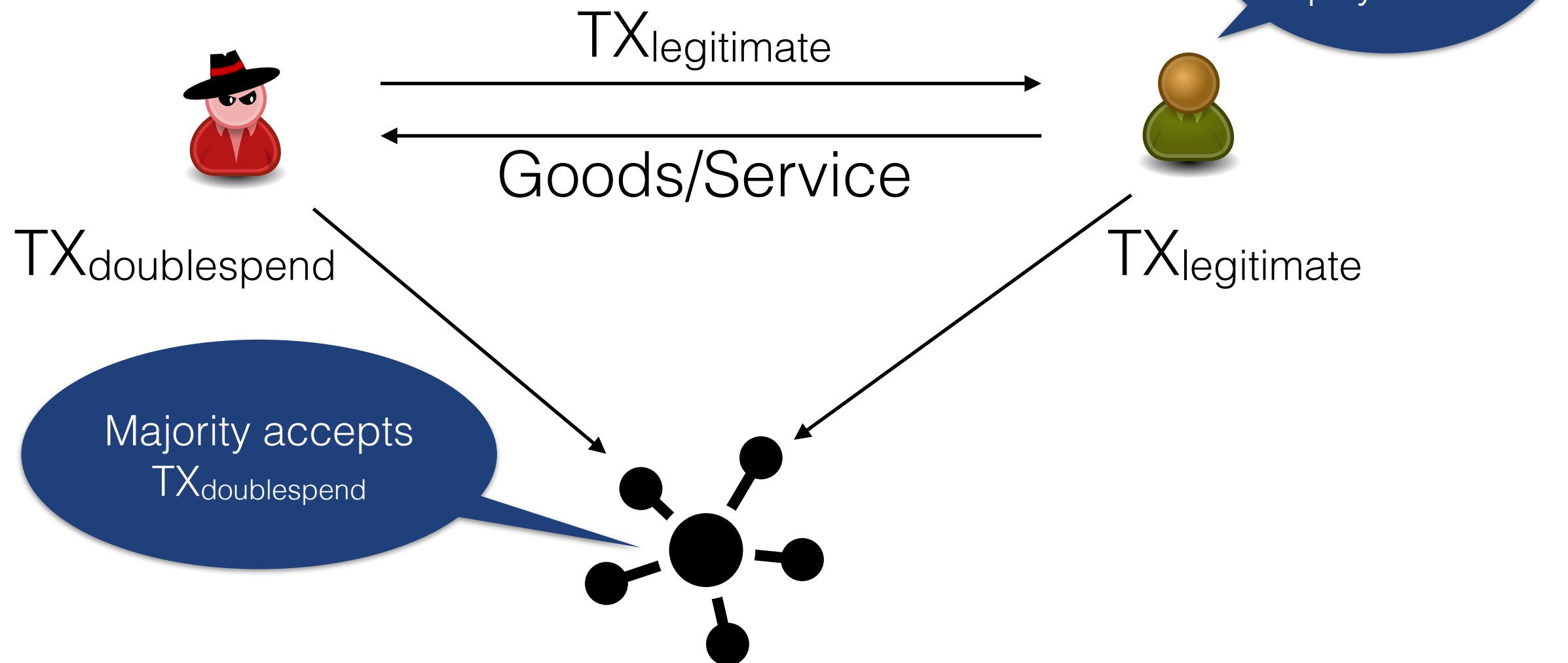$TX_{doublespend}$

$TX_{legitimate}$

Majority accepts $TX_{doublespend}$

What is Double Spending?

Spending money more than once

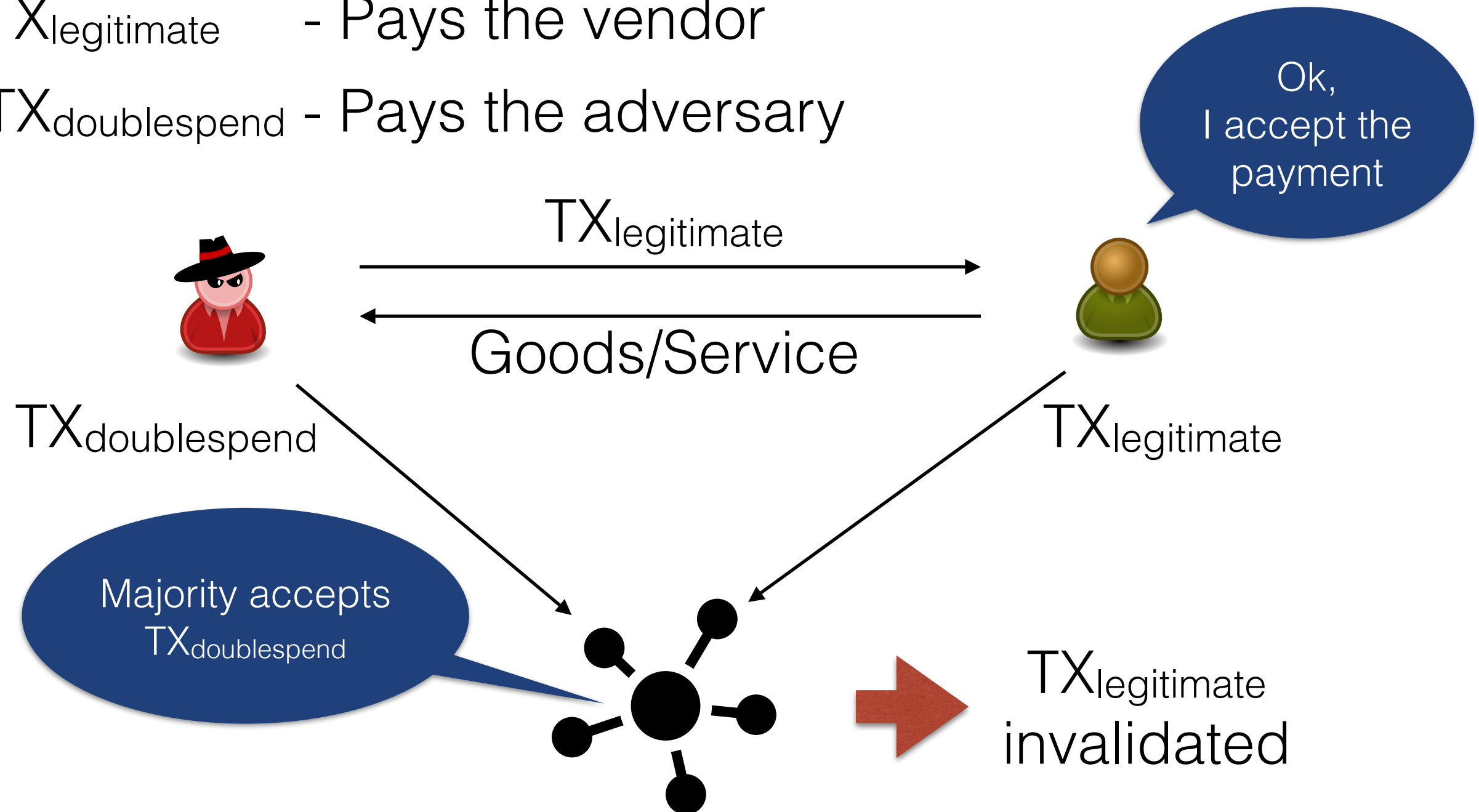$TX_{legitimate}$ — Pays the vendor

$TX_{doublespend}$ — Pays the adversary

$TX_{legitimate}$

Goods/Service

Ok, I accept the payment

$TX_{doublespend}$

$TX_{legitimate}$

Majority accepts $TX_{doublespend}$
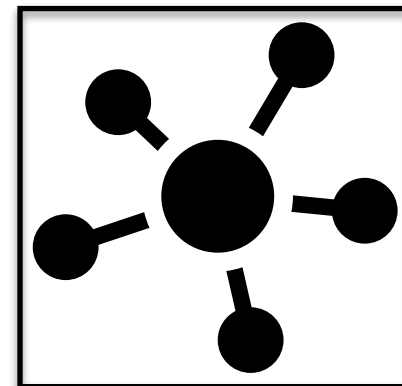
$TX_{legitimate}$ invalidated

2

Double Spending 0 Confirmation Transactions

- Very reliable attack

- Regardless of protection (double spend relay)

Vendor

Bitcoin Network

Double Spending 0 Confirmation Transactions

- Very reliable attack

- Regardless of protection (double spend relay)

Blind TX$_{doublespend}$

Vendor

Bitcoin Network

Double Spending 0 Confirmation Transactions

- Very reliable attack

- Regardless of protection (double spend relay)

Blind TX$_{doublespend}$

Vendor

TX$_{doublespend}$
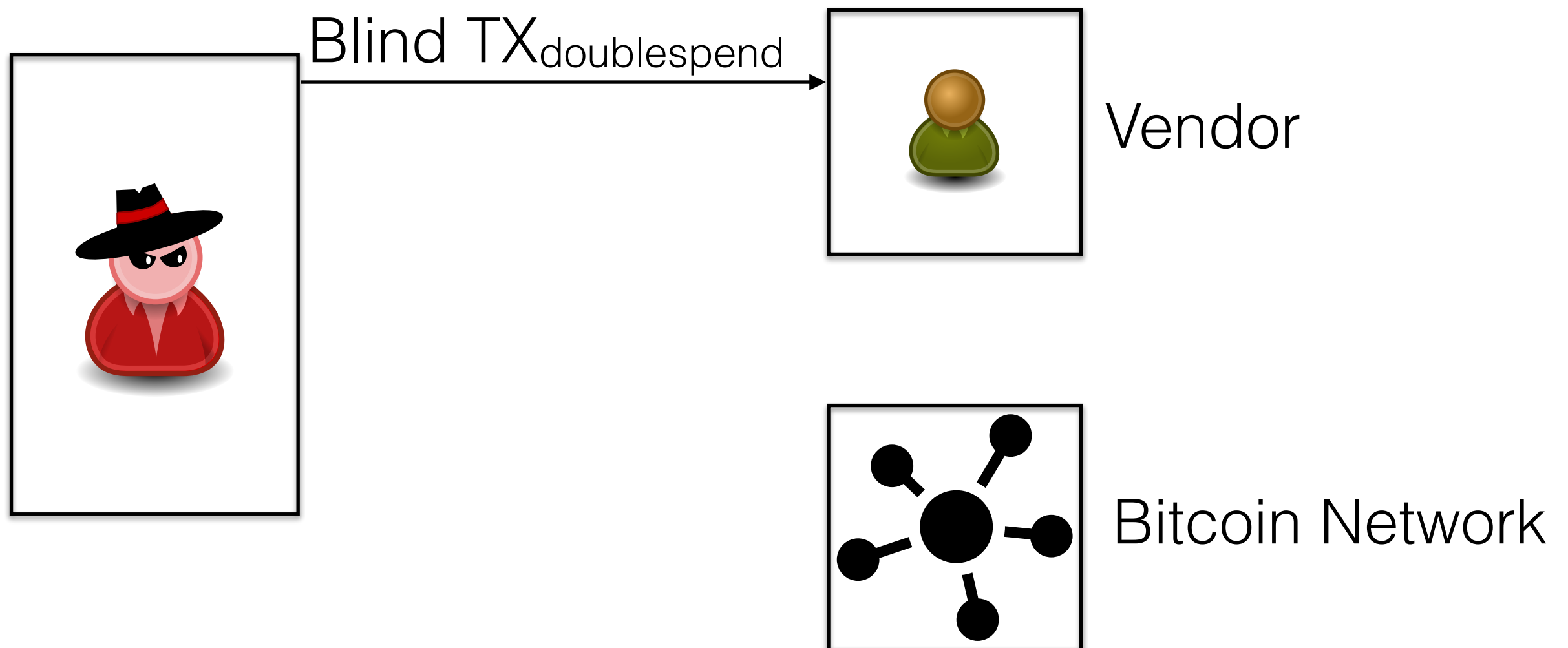
Bitcoin Network

Double Spending 0 Confirmation Transactions

- Very reliable attack

- Regardless of protection (double spend relay)

Blind $TX_{doublespend}$
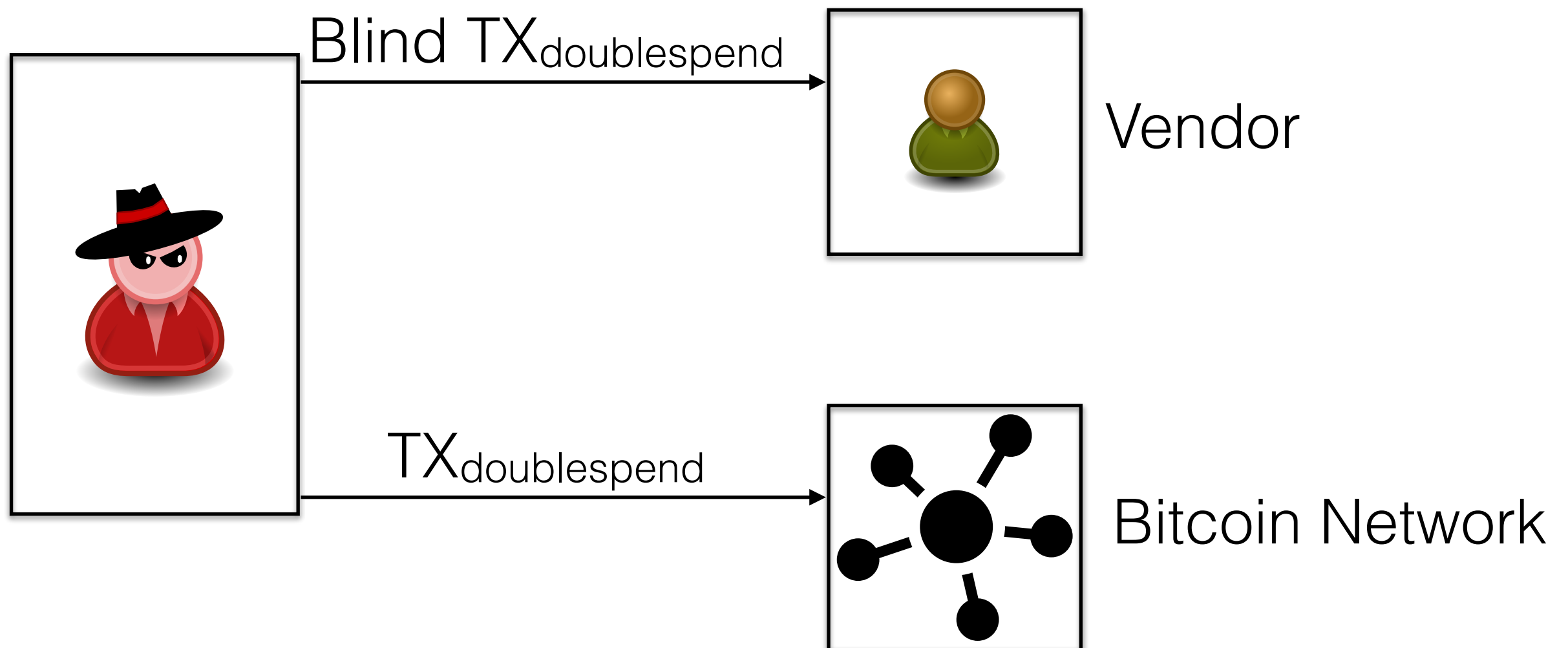
Vendor

Advertise $TX_{doublespend}$

$TX_{doublespend}$

Bitcoin Network

Double Spending 0 Confirmation Transactions

- Very reliable attack

- Regardless of protection (double spend relay)

Blind $TX_{doublespend}$

$TX_{legitimate}$

Vendor

Advertise $TX_{doublespend}$

$TX_{doublespend}$

Bitcoin Network

Double Spending 0 Confirmation Transactions

- Very reliable attack
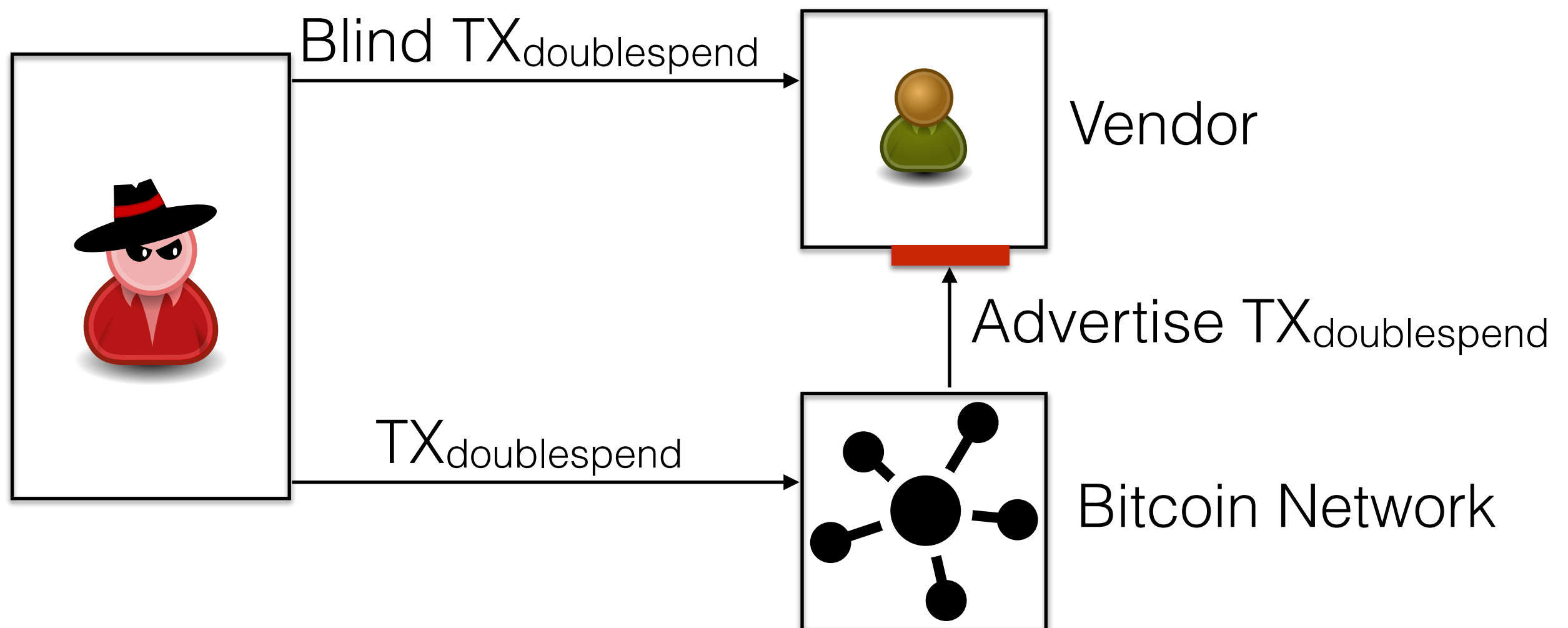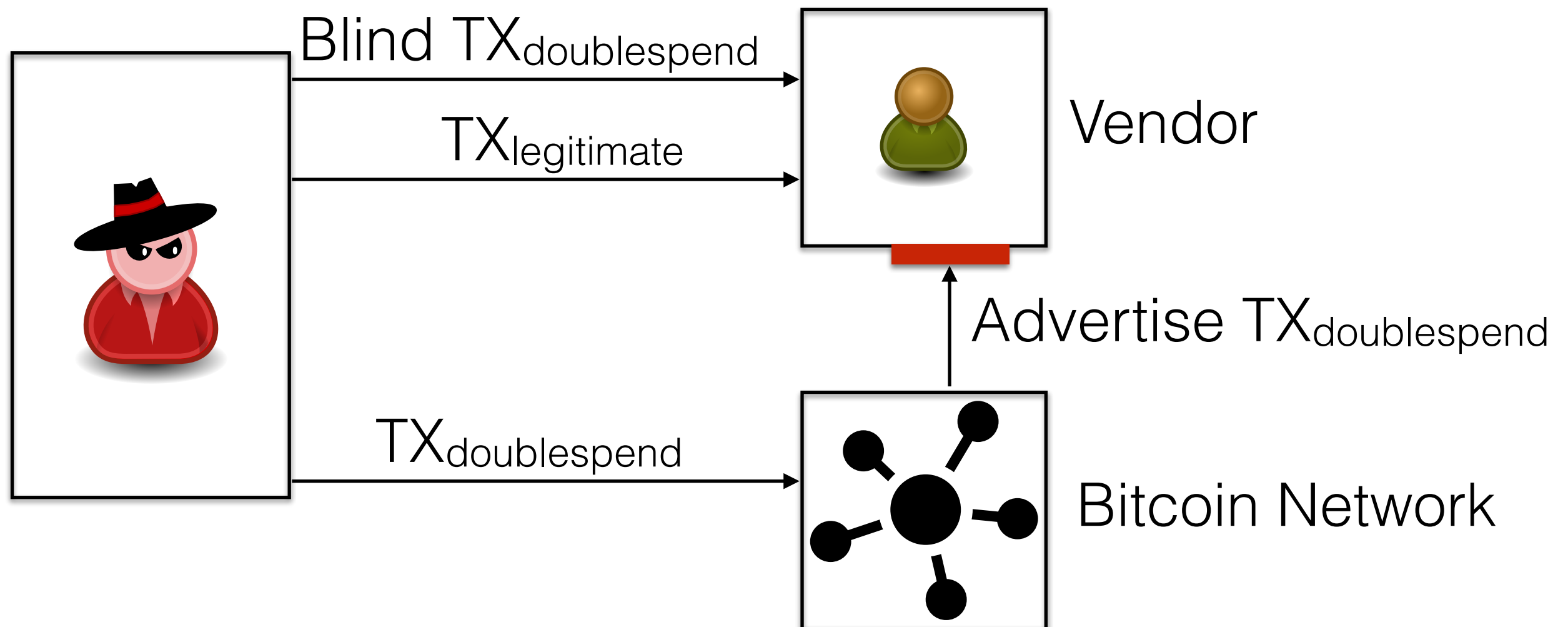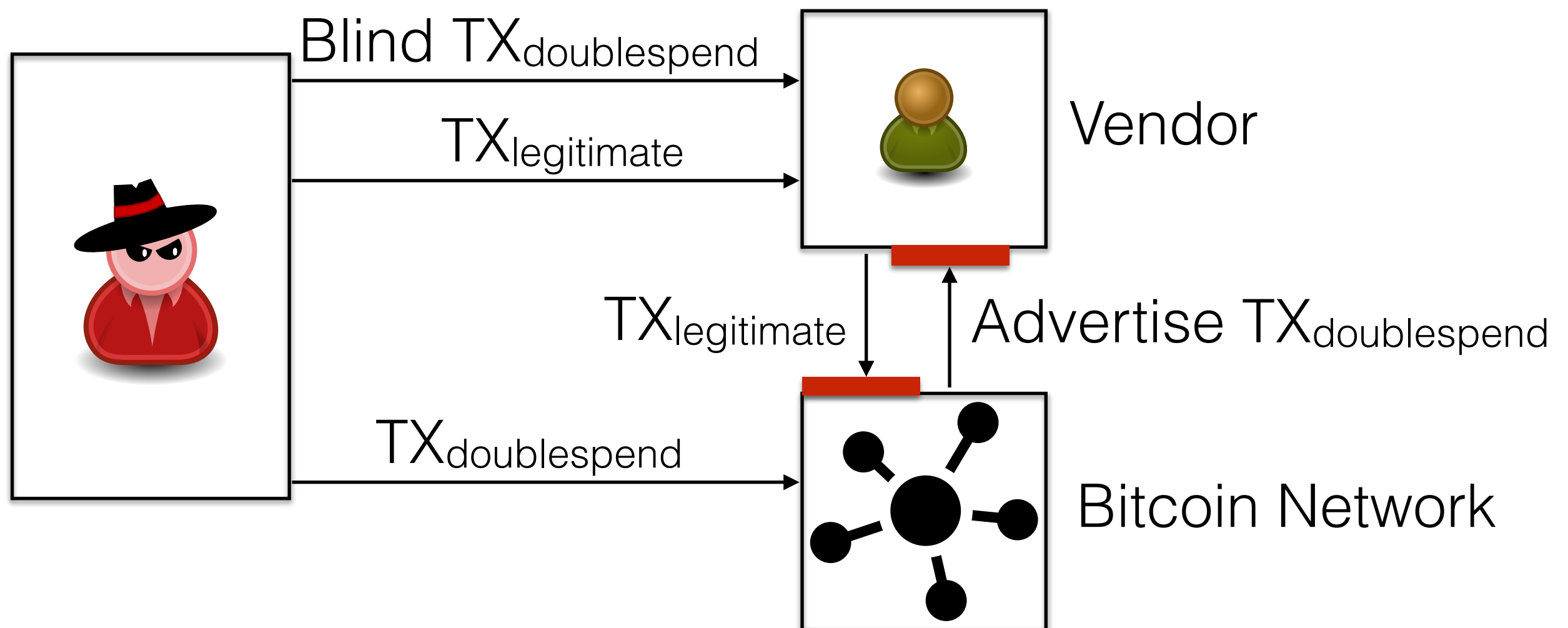
- Regardless of protection (double spend relay)

Blind $TX_{doublespend}$

$TX_{legitimate}$

Vendor

$TX_{legitimate}$

Advertise $TX_{doublespend}$

$TX_{doublespend}$

Bitcoin Network

3

Implications - Double Spending 1 Confirmation Transactions

1. Withhold T_d
7. Withhold B_d
11. Send B_l

Vendor

2. Withhold T_d
4. Send T_l
8. Withhold B_d
10. Send B_l

Weak Miner

9. Mine B_l

3. Send T_d
6. Send B_d

Bitcoin network

5. Mine B_d

Adversary

X**l** = legitimate
X**d** = double spend attempt