Payments and double spending

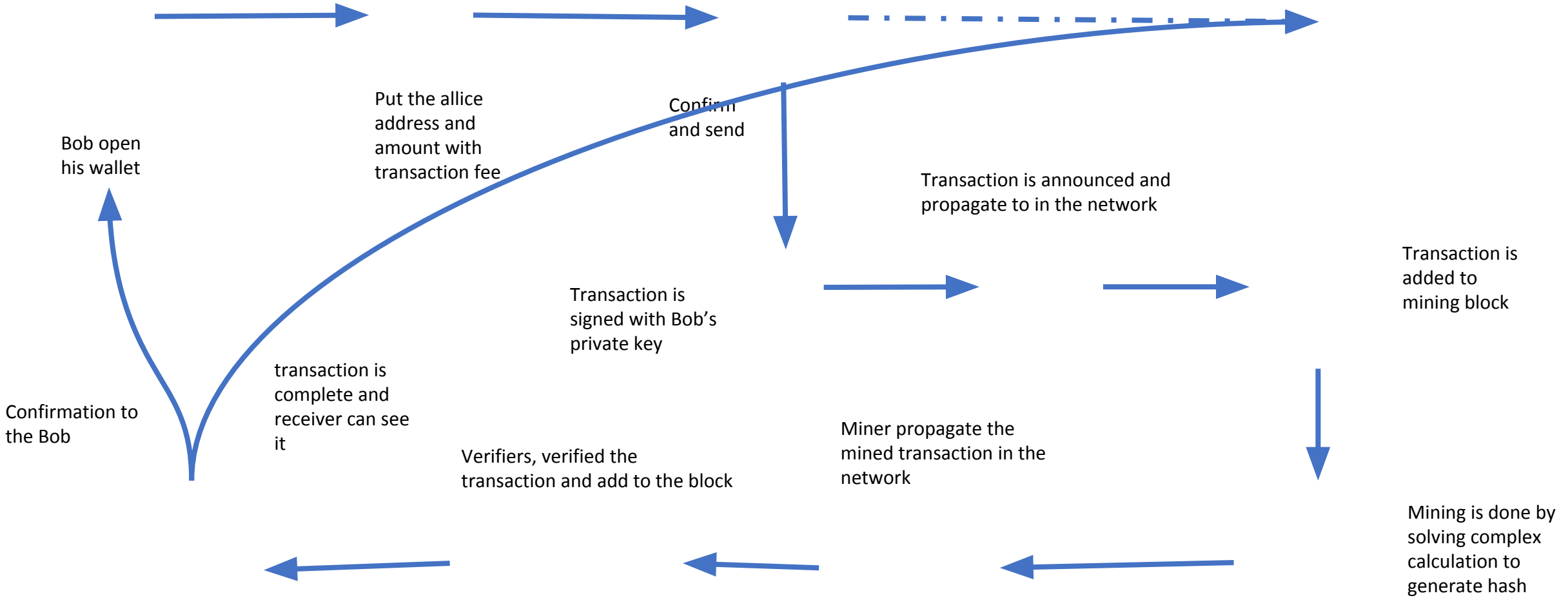
Dr. Preeti Chandrakar
Assistant Professor

Department of Computer Science and Engineering
National Institute of Technology, Raipur
September 2021

Outline

- Introduction
  - Payment in bitcoin network(transaction)
  - Double spending
- Types of double spending attack
- Working of Double-spending Bitcoin
- Effect of Double Spending on Blockchain
- Prevention from double spending

Introduction: Payment in bitcoin

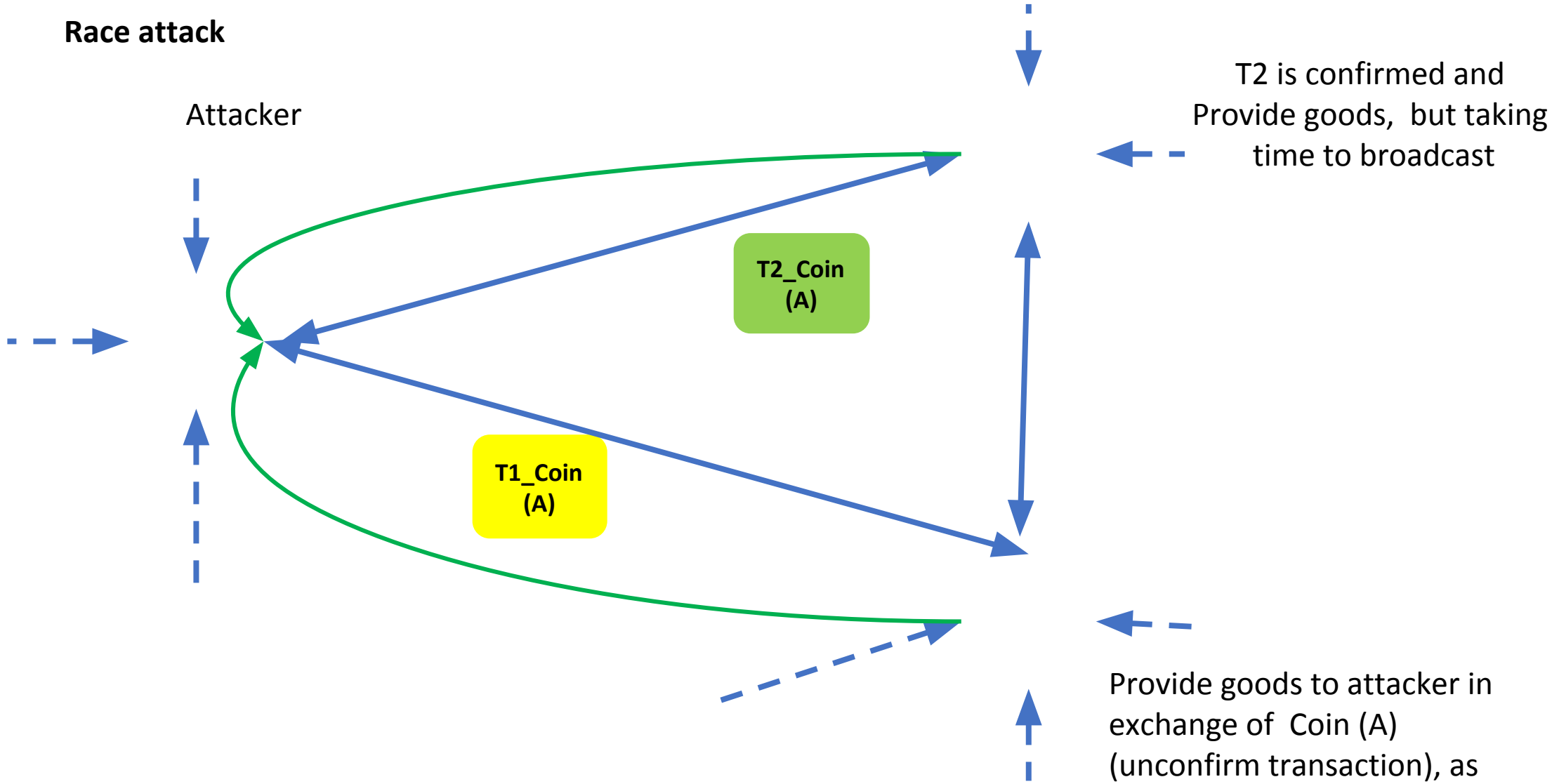


Introduction: Double spending

- The double spending problem is a phenomenon in which a single unit of currency is spent simultaneously more than once
- This creates a disparity between the spending record and the amount of that currency available
- Transaction information within a blockchain can be altered if specific conditions are met
- The conditions allow modified blocks to enter the blockchain
- if this happens, the person that initiated the alteration can reclaim spent coins.

Types of Double-Spending Attacks

Race attack



Working of Double-spending Bitcoin

- A bad actor sending a copy of one transaction to make the copy appear legitimate
- And same time retaining the original, or erasing the first transaction.
- There are a few different ways criminals attempt to double-spend Bitcoin

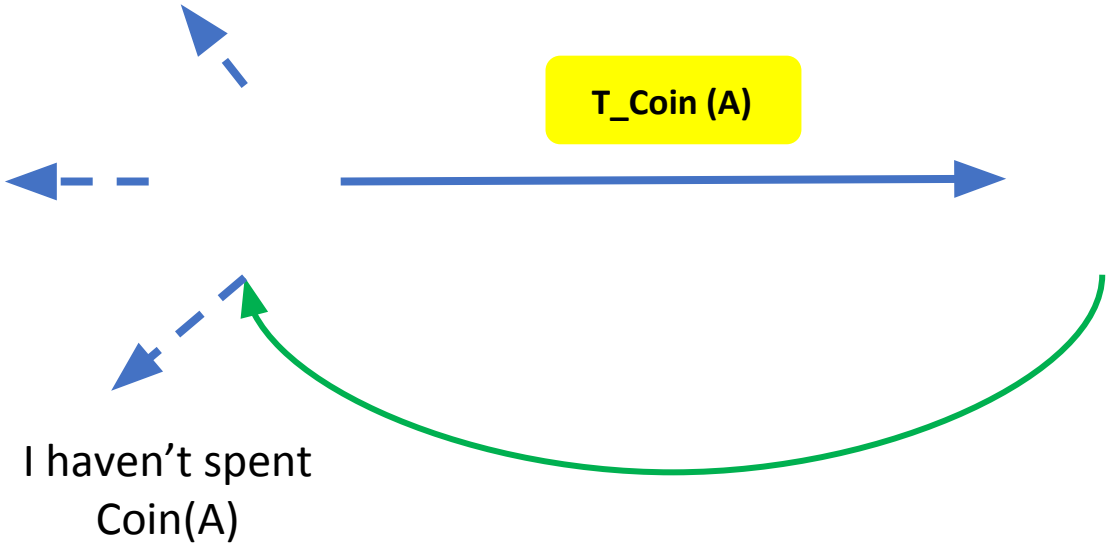
A. Simultaneously Sending the Same Bitcoin Amount Twice (or More)

- An attacker will simultaneously send the same bitcoin to two (or more) different addresses
- This type of attack attempts to exploit the Bitcoin network's slow 10-minute block time
- in which transactions are sent to the network and queued to be confirmed and verified by miners to be added to the blockchain.
- In sneaking an extra transaction onto the blockchain,
- Thieves can give the illusion that the original bitcoin amount has been not spent to support the desired future double spend.

How Does Double-spending Bitcoin Work

B. Reverse an already-sent transaction

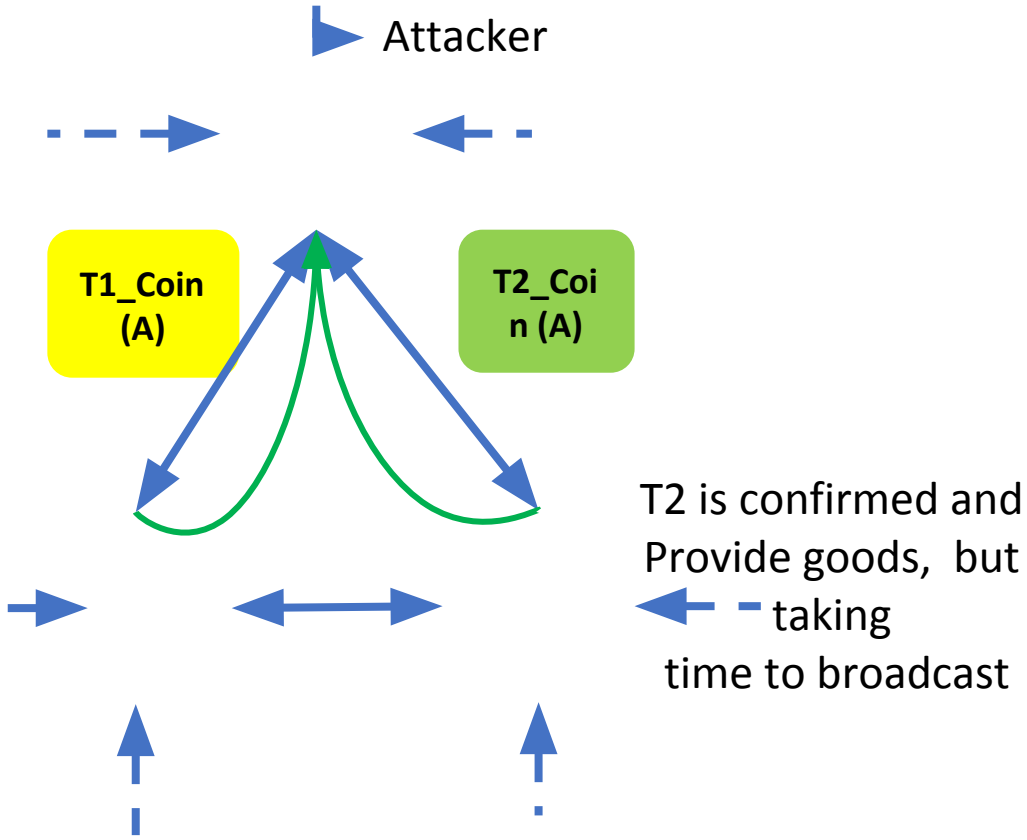
- Another way to attempt a Bitcoin double-spend is by reversing a transaction
- After receiving the counterparty's assets or services, transaction is revers
- Thus keeping both the received goods and the sent bitcoin.
- The attacker sends multiple packets (units of data) to the network to reverse the transactions, to give the illusion they never happened.



Transaction is confirmed and Provide goods

Types of Double-Spending Attacks

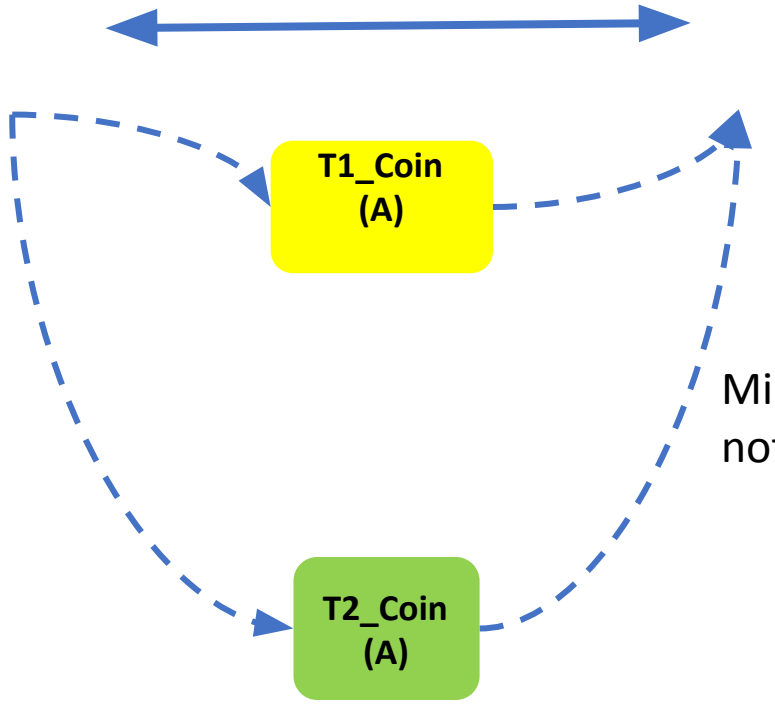
Race attack



T2 is confirmed and Provide goods, but taking time to broadcast

Provide goods to attacker in exchange of Coin (A) (unconfirm transaction), as T2 isn't broadcast

Finney attack

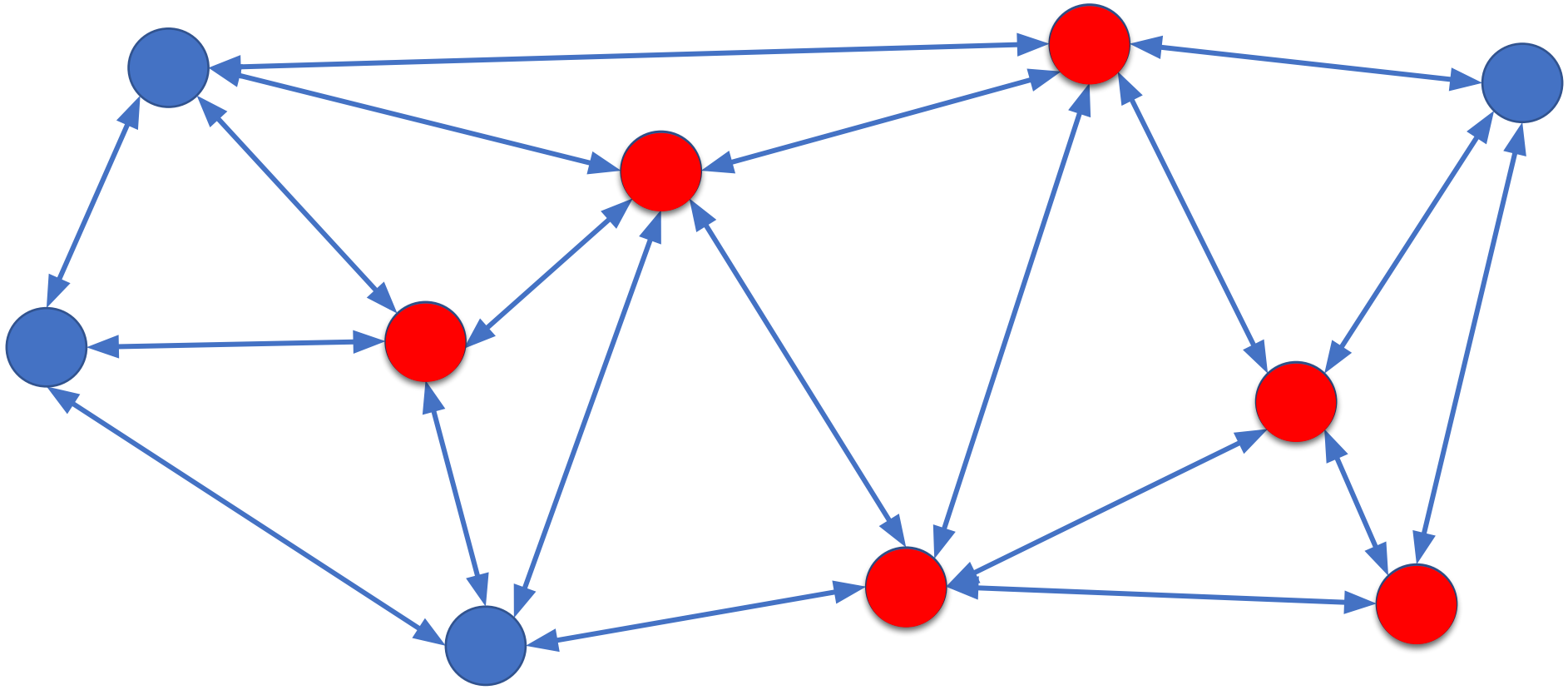


Mined T1, but not Broadcast

Mined T2, And Broadcast T2 and T1

Finney attack is possible only if the recipient accepts an unconfirmed transaction

Types of Double-Spending Attacks



A **51% attack** occurs when a group of individuals controls more than 50% network

Effect of Double Spending on Blockchain

- Double spending affect the ledger that two transaction log is generated,
- a fake one for seller and another one for the network.

- If anyone get 51% of control to the network then they can:
  - Control the network and Modify the ledger
  - And transfer bitcoin to their digital wallet multiple times
  - As if the original transactions had not yet previously occurred

- Due to decentralized system its hard to control the double-spending of cryptocurrency

How Does Bitcoin Prevent Double Spending?

- Bitcoin’s proof-of-work consensus model is inherently resistant to double-spending because of its block time.
- Proof-of-work requires miners on the network, or validator nodes, to solve complex algorithms
- that require a significant amount of computing power, or “hash power.”
- This process makes any attempt to duplicate or falsify the blockchain significantly more difficult to execute,
- While it is technically possible for a group of individuals to initiate a 51% attack on the Bitcoin network,
- Successfully executing a 51% attack has only gotten more difficult over time,