NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

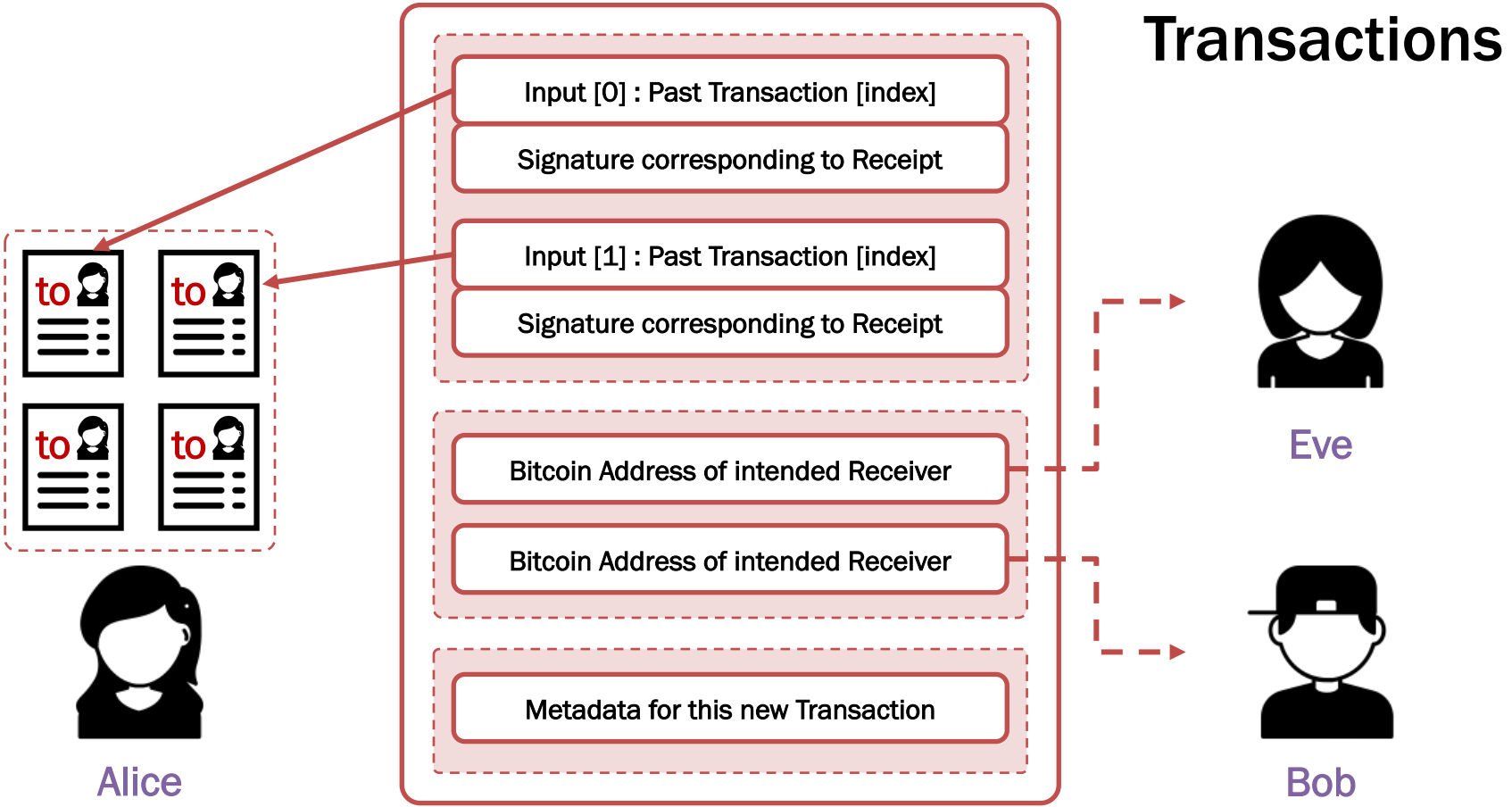
Tutorial

# Bitcoin Transactions

CE/CZ4153

Blockchain Technology

# Transactions



# Question 1

Ref : Week 2 Lectures

How would you securely store each of the following if you own a digital asset like Bitcoin -- Private Key, Public Key, Address? What if you lose them?

# Question 2

Ref : Week 2 Lectures

Suppose Alice creates a transaction for Eve and Bob. Total input is 2 BTC, Eve gets 0.5 BTC and Bob gets 1.5 BTC. If Eve tries to use this transaction as input to her own transaction later, can she spend both her and Bob's share, that is, the total 2 BTC?

# Question 3

Ref : Week 2 Lectures

In a Bitcoin transaction, if

Sum( input Satoshi ) > Sum( output Satoshi ),

what happens to the balance/remaining Satoshi value Sum( input Satoshi ) - Sum( output Satoshi )?

# Question 4

Ref : Week 2 Lectures

If Coinbase Transactions can "generate" Bitcoin through mining, what should be the restrictions on such Coinbase Transactions such that there is no artificial inflation in the economy?

# Question 5

Ref : Week 3 Lectures

Can you run a Bitcoin Node just to receive/create Transactions? Do you have to take part in Validation and Recording of other Bitcoin Transactions?

How many types of Nodes can there be in Bitcoin?

# Question 5

Ref : Week 3 Lectures

Which nodes in the Bitcoin network (or the extended network) store a copy of the Full Blockchain?

- Bitcoin Core
- Full Blockchain Node
- Wallets with Payment Verification
- Mining Nodes

# Question 5

Ref : Week 3 Lectures

Suppose you want to verify your own transactions on the bitcoin blockchain, but you do not care about verifying anyone else's transactions.

- Do you need to store the full blockchain?
- If not, what are the bare minimum components from the blockchain that you need to store?