MarketPeer

A P2P Digital Market Platform

Yifei Li, Liangyong Yu, Lin Yuan

Introduction

- P2P Digital Market Platform, with digital currencies and digital assets
- DHT: store metadata
- Ethereum-alike blockchain: regulate transaction executions
- Smart Contract: without need of trusted third party

Yifei Li
Blockchain

Liangyong Yu
DHT

Lin Yuan
Smart Contract

Chord: implementation of distributed hash table

Functionality: store product information and account information for blockchain

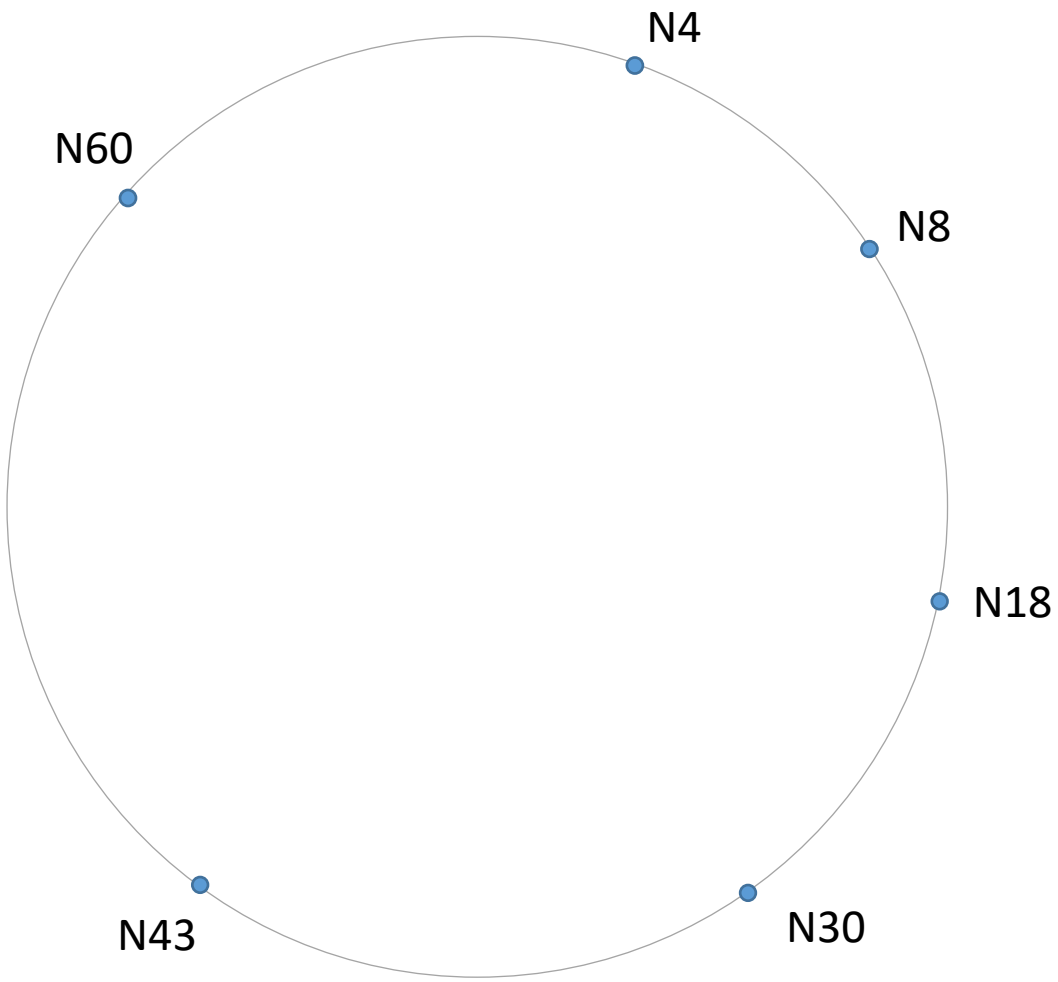
API:

1. Put(k,v): store a key-value pair into Chord
2. Lookup(k): find which node owns the key
3. Get(k): read a value from Chord based on key

Liangyong Yu

The structure of Chord: predecessor and successor

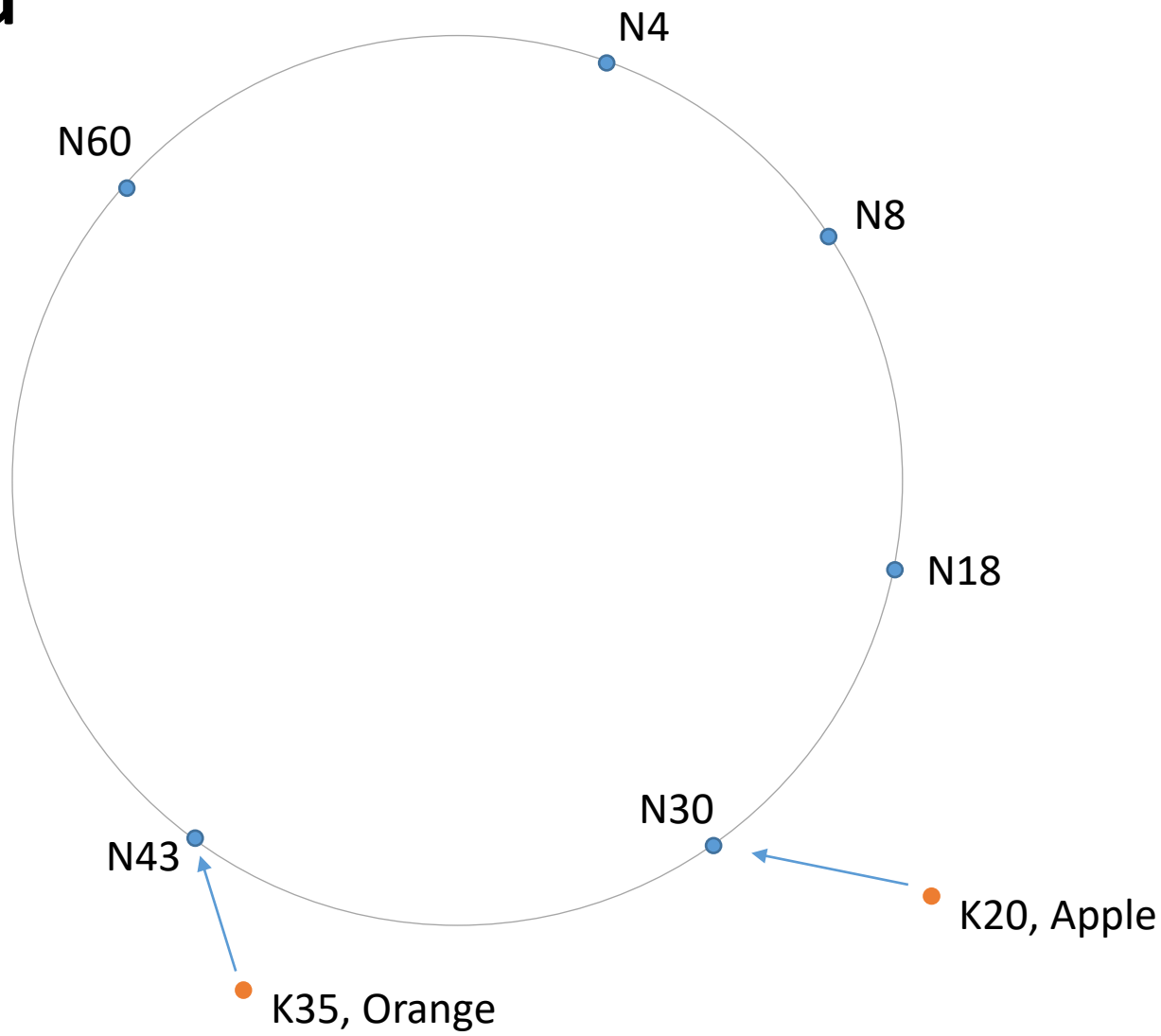
hash a node to an address [0, 64)



node	predecessor	successor
N4	N60	N8
N8	N4	N18
…	…	…

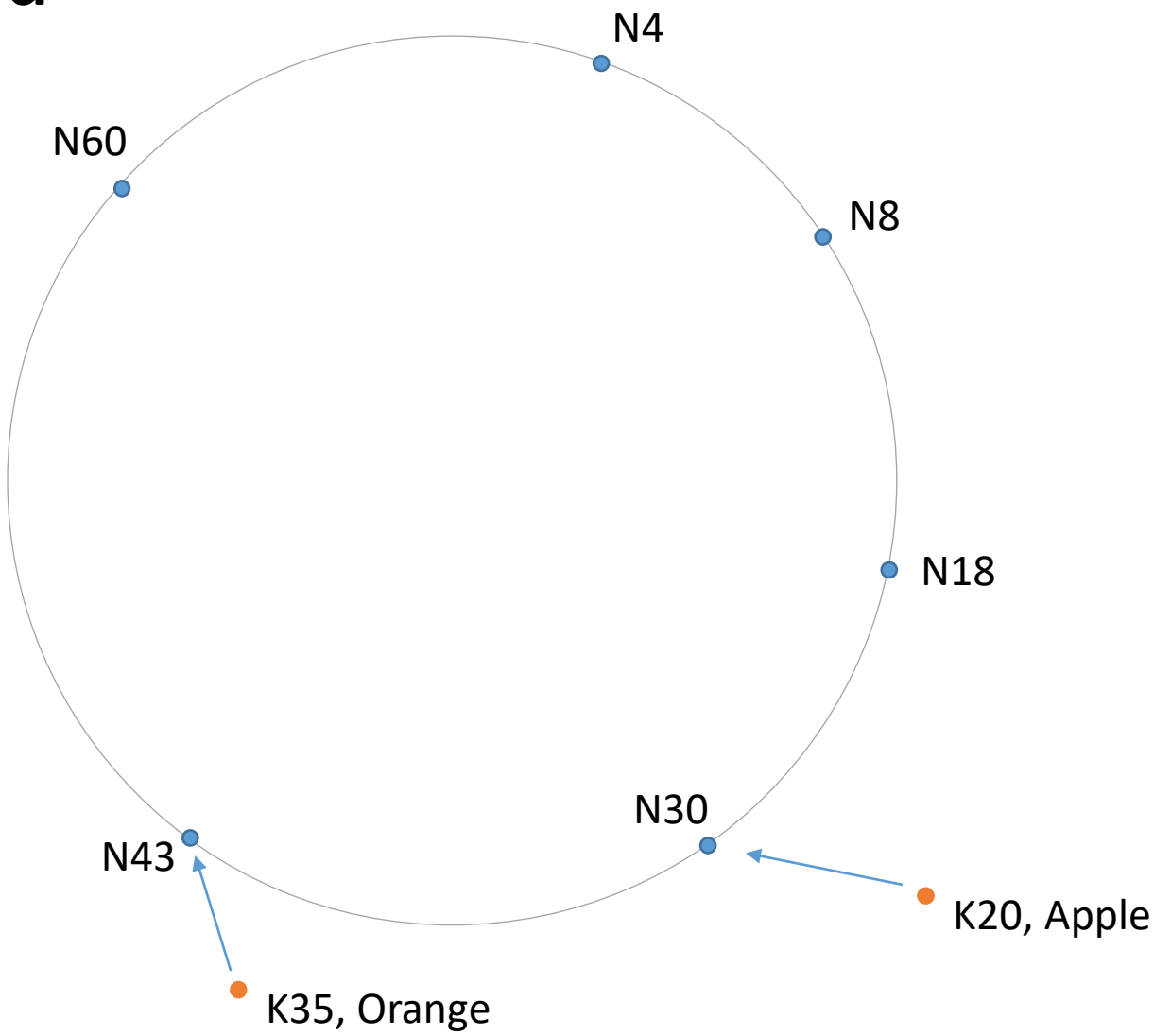
Put a key-value pair into chord

N4.put(20, Apple):
find the successor of 20



Get a key-value pair into chord

Apple = N4.Get(20)



Liangyong Yu

Add new node into the chord system

N36.Join(N4):

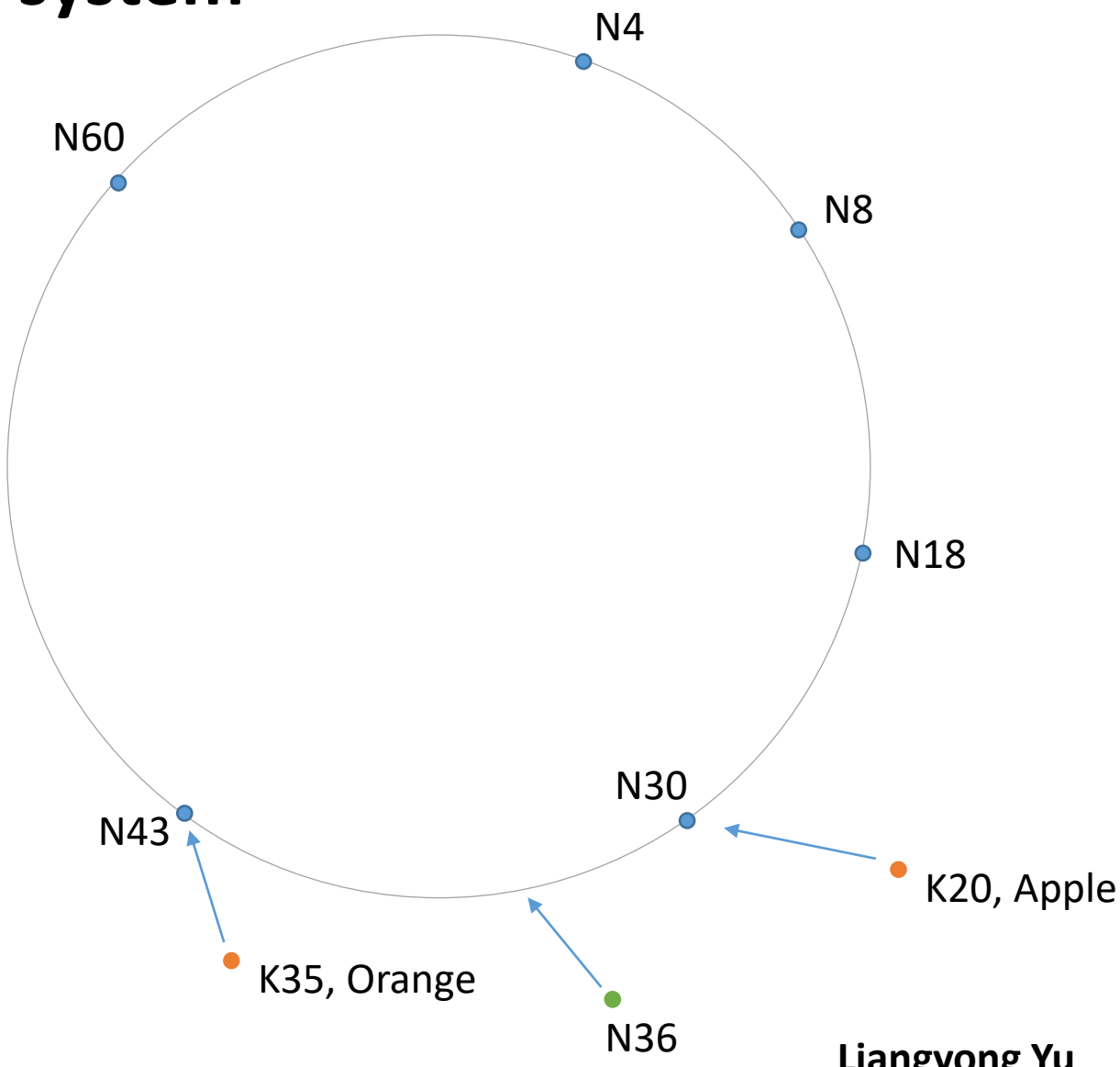
1. find the underlying successor of N36
2. add N43 as successor
3. invoke Stabilize() and FixFingerTable() periodically

N36.Stabilize():

notify successor to its existence periodically

N36.FixFingerTable():

update its finger table

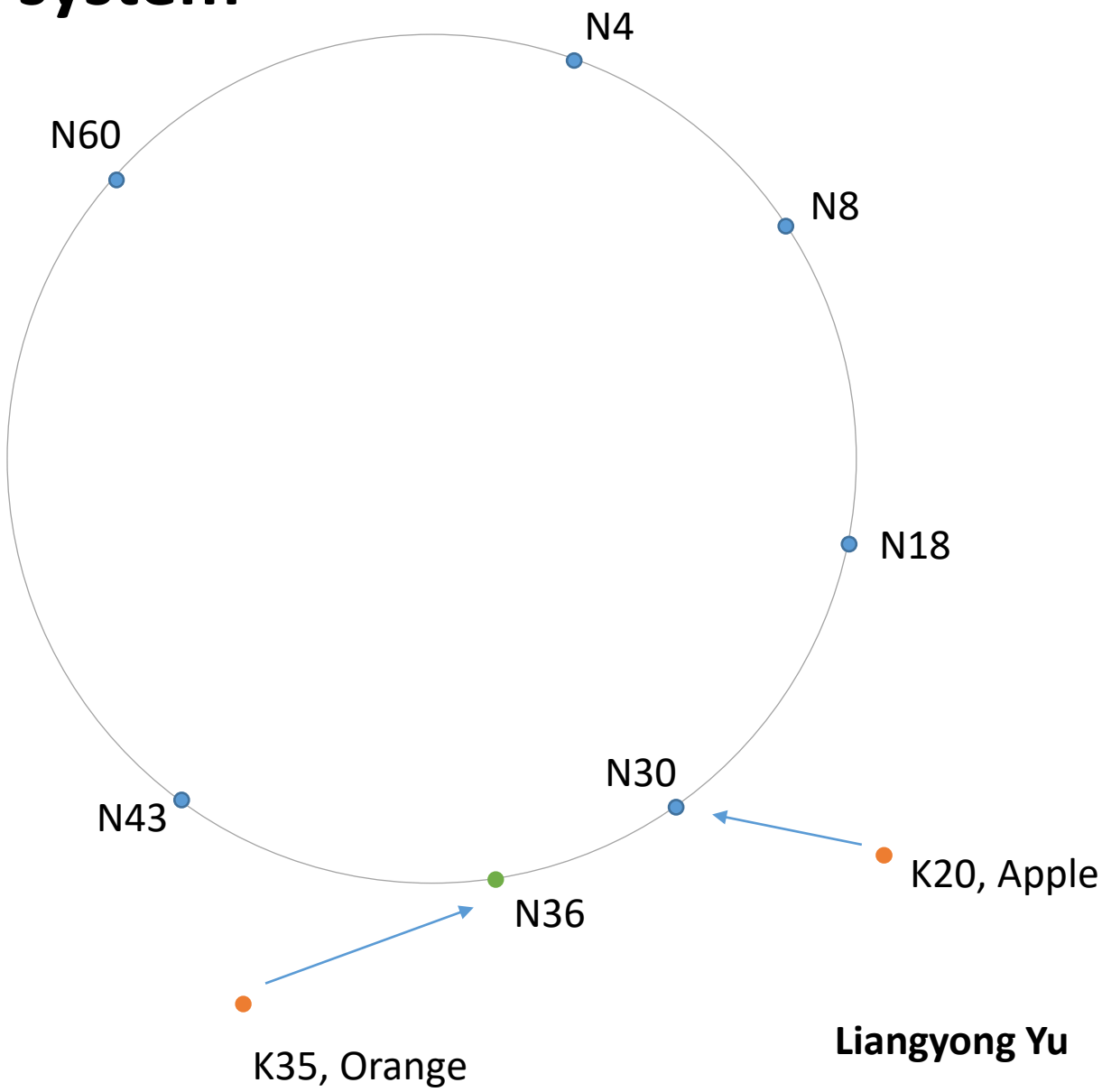


Liangyong Yu

Add new node into the chord system

N36.Join(N4):

transfer the old key into the new joined node



Liangyong Yu

Ethereum-like Blockchain

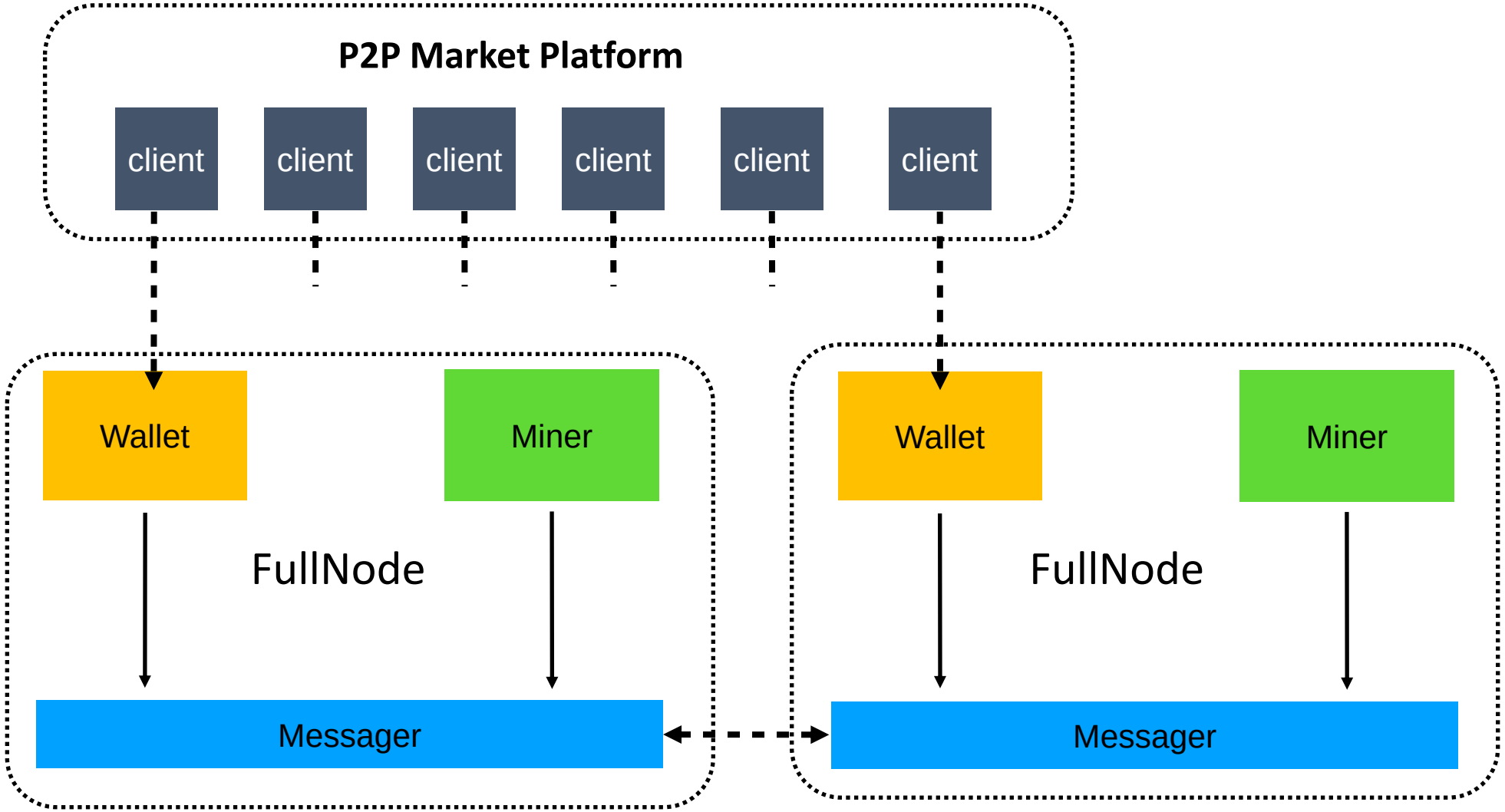
Why?

- Why using *blockchain*?
  - manage ***digital currencies***
  - validate and regulate the transactions with an ***immutable "ledger"***
- Why *ether-like*?
  - fine-grained and ***explicit world state*** -> manage ***digital assets***
  - ***smart contract*** -> regulate behaviors between buyers and sellers

Yifei Li

System Architecture

Overview



Yifei Li

System Architecture

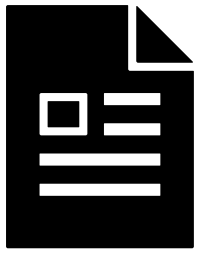
wallet

client

Account: 0x7egq…

Balance: 1340 Epfer

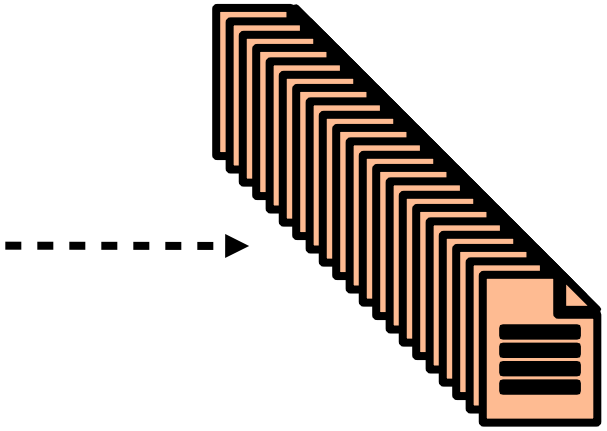
Storage: {apple: 100, orange: 200}



Smart Contract:

If A sends B 1 apple,
B sends A 100 Epfer

- Entry point to the Epfer Network
- SyncAccount
- TransferToken
- ProposeContract
- TriggerContract

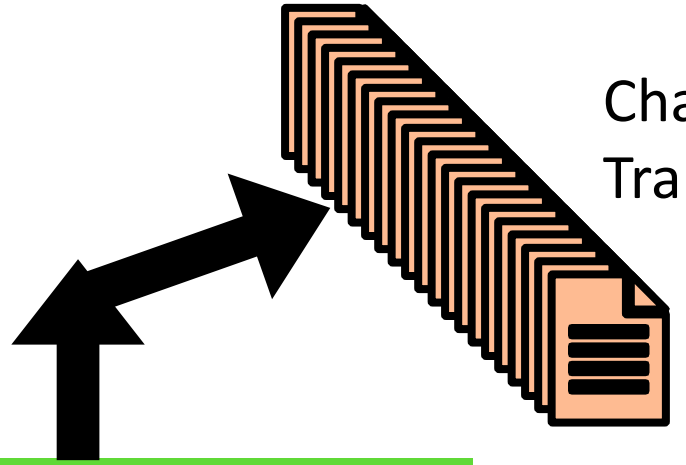


Chain of Transactions

Yifei Li

System Architecture

miner



Chain of Transactions

Miner

Miner

Wallet

Wallet

- Vital components of the EpferNet
- Verify the transactions
- Generate new block based on bitcoin-style PoW
- Verify the block sent by other miners

Wallet

Miner

Wallet

Miner

Yifei Li

Smart Contract: Simplified of Ethereum

- Solidity: Turing-complete Programming Language
- If-Action: Minimum set of primitives

- EVM: Compiled bytecode in VM (**isolated** from network, file system…)
- Interpreted Execution: AST to Transaction

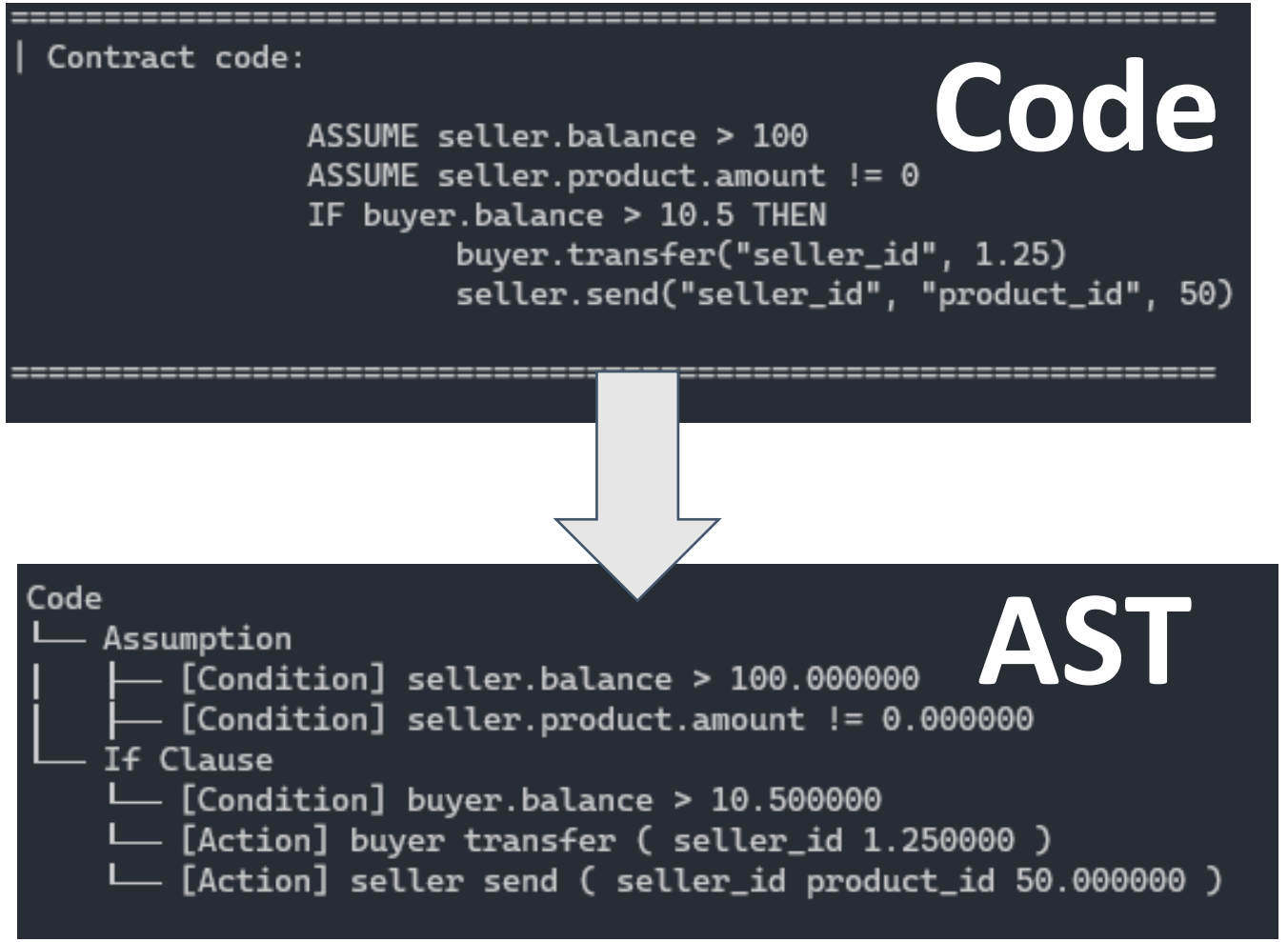
- Immutability, global distributability supported by underlying blockchain

Lin Yuan

If-Action: Contract Code

- **ASSUME**: preconditions
- **IF Clause**: condition + actions

- **Parse** Code to AST
- Replace reserve words
  - Role: Buyer, Seller
  - Action: Transfer, Send



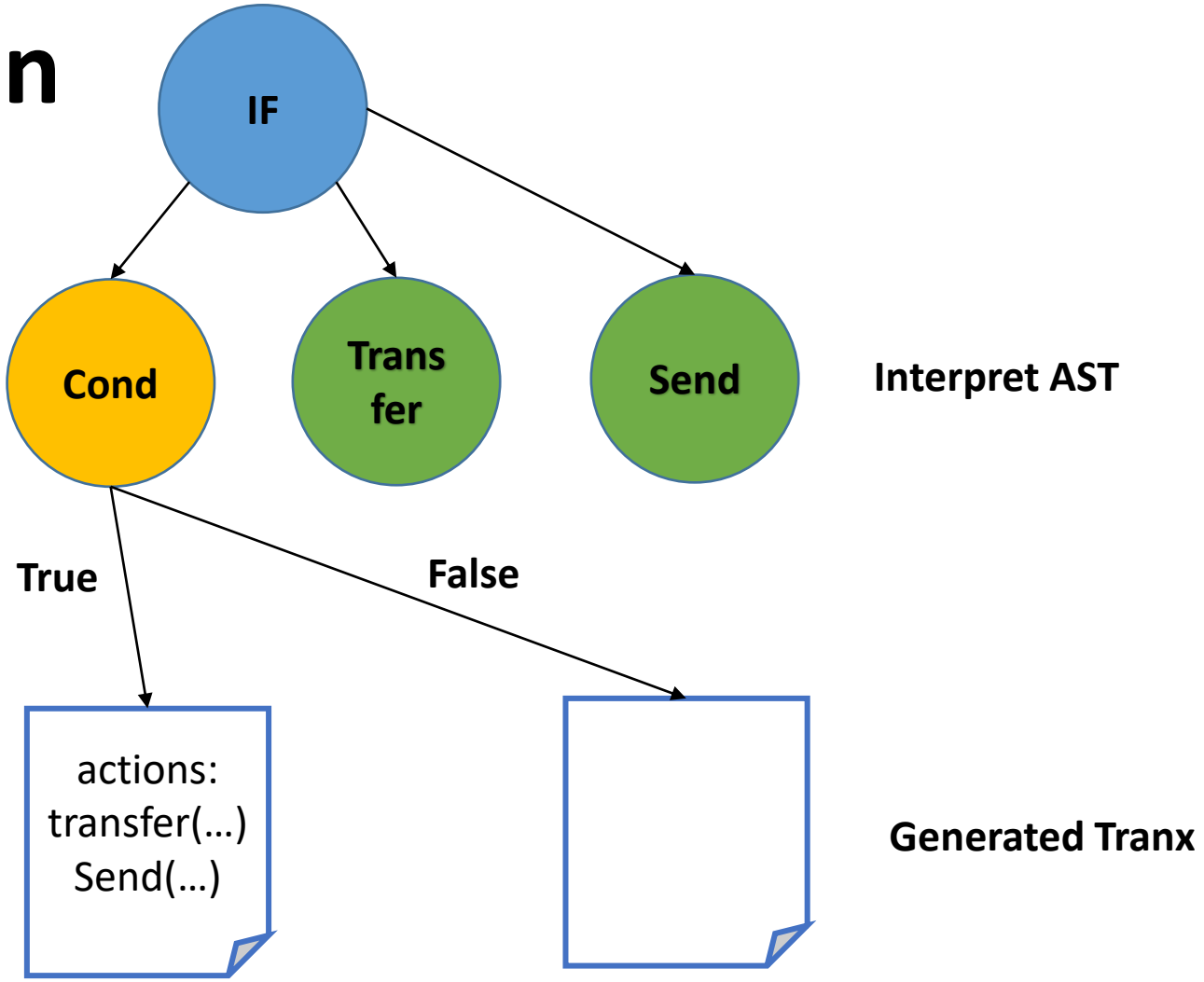
Lin Yuan

Contract Preparation

- Simply **interpret** AST

- Package satisfied actions

  → Blockchain Tranx



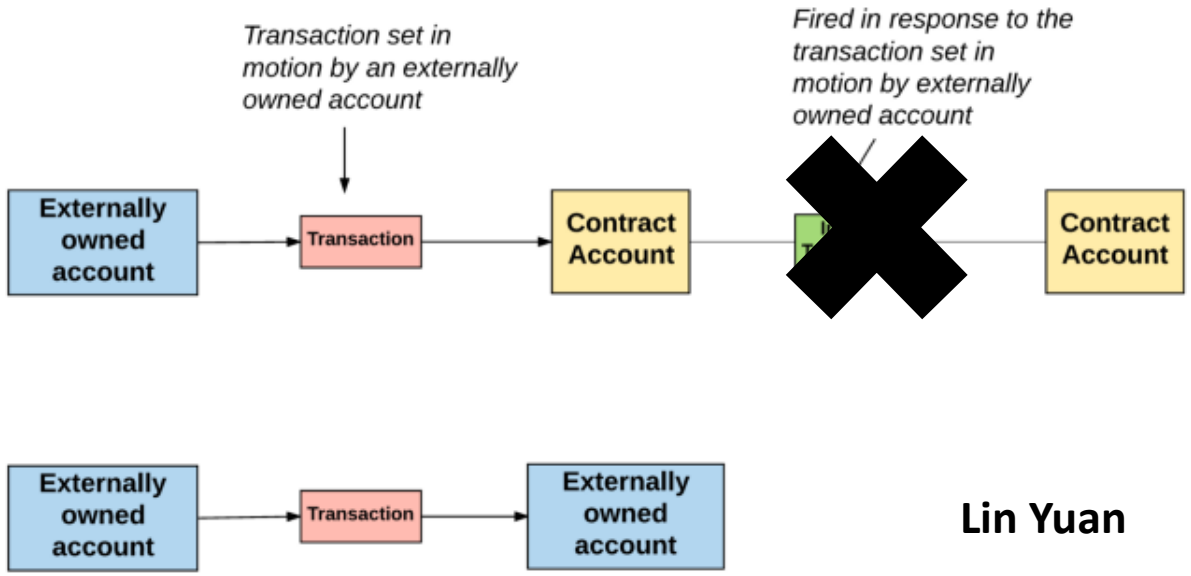
Lin Yuan

Contract Execution

- Transaction Execution

  == State transition

- 1. Proposer create contract
- 2. Message to Acceptor
- 3. Acceptor execute contract
- p.s. Miners trying to submit tranx



Lin Yuan