

①
5/6/2019

① Make sure Submit command works for you!

②

Q1: Design representation

Contract diagram

"Static" structure

finite state machine
FSM
"dynamics"



← users ← identity ← account addresses
← assets
← roles ← member chair

← rules

← constructor
← register ← "escrow" self
← unregister ← chair
← payment settlement ← Consortium leader

← other functions
important: need to be recorded on the block chain

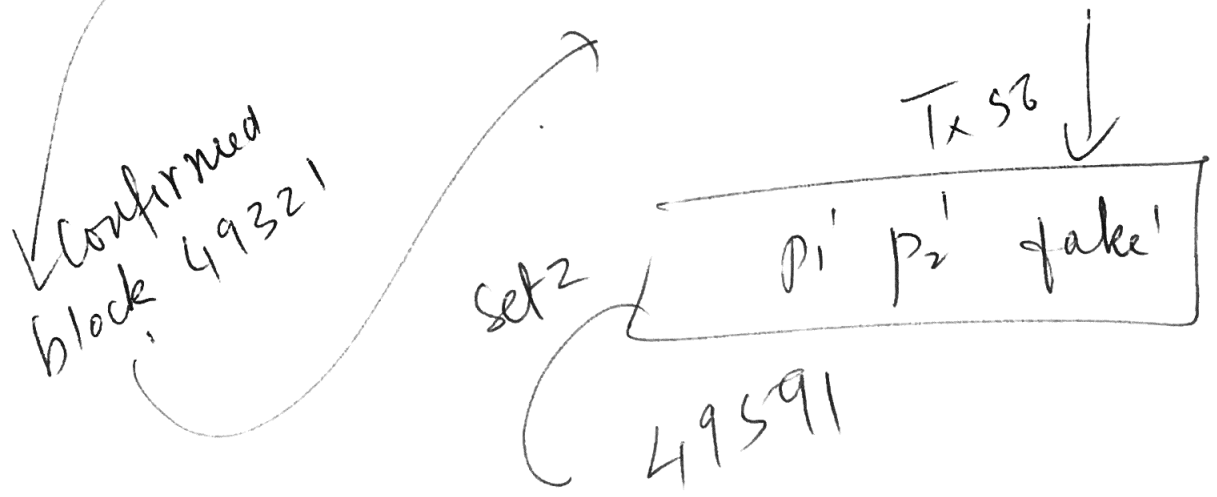
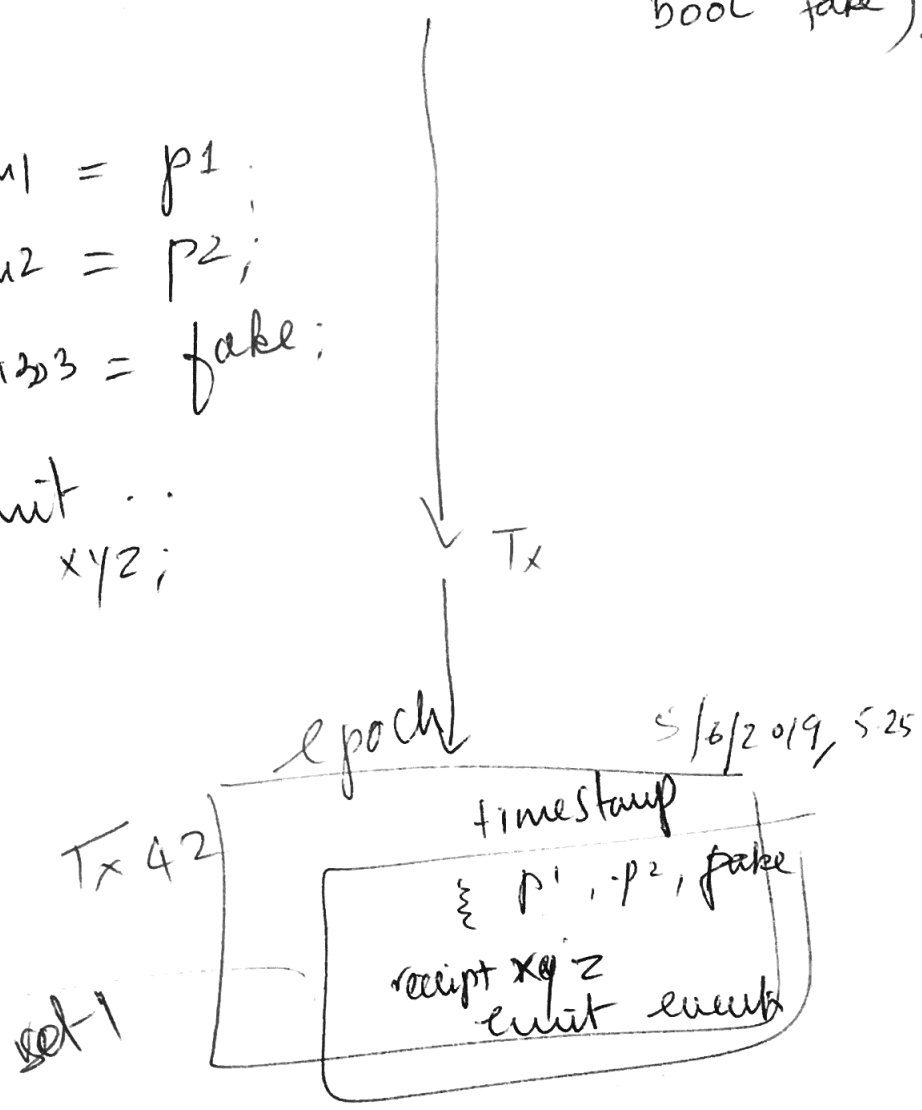
↑ internal ↑ view function

Safe Purchase
Example
Read the
docs
Solidity

5/6/2019
②

function example (uint p1, bytes32 p2,
bool fake)

```
{  
    myparam1 = p1;  
    myparam2 = p2;  
    myparam3 = fake;  
    emit ...  
    return xyz;  
}
```



③
5/6/2019

① Simple data type

asset

roles

uint

bytes32

bool

struct

address

mapping

enum

(multiple mapping)

→ phases of SC

② Rules

Safe Purchase example

modifiers

how to define
modifiers

usage → . function
headers

modifier name (parameter)
{ require (expression with parameter);
— ;
}

what is the
diff?

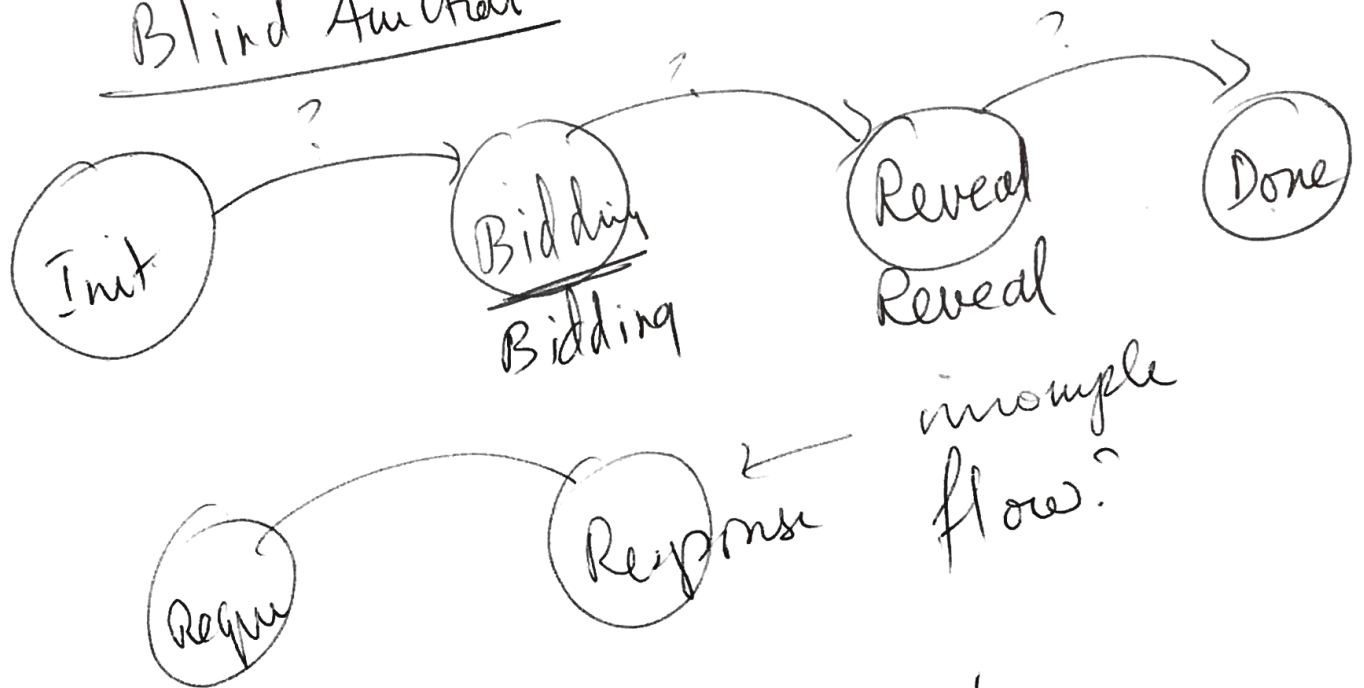
~~require (age $\geq$ 21);
if (age $\leq$ 21) return;~~

assert (noOfpeople == count);
"failing"

a) contract diagram

b) FSM finite state machine

Blind Auction



25%

25% Problem statement → Smart contract Code

50%

~~events~~ +

Event: Definition of event
emit of events
? how to handle emitted events

10

web3 : Standard library
Bina's slides web3
Read the docs

10-15

what is it? How is it used?
"demo"

web3.eth
web3.net

10. Lab2 directory structure "Standards"
baffle created

Standards + model Dapp
ERC 20 ERC 721

10. 8.

Block → Tx → consensus

5.

Web3
Demo

(1) Problem
statement
FSM
contract
Diagram
and