

Theory of Blockchain



Session 9:

Ethereum – Part 1

Module 1 – Ethereum Core Idea

Bitcoin is not Alone

- There are plenty of other cryptocurrencies

- Monero
- Litecoin
- Zcash
- Ripple
- IOTA (tangles)
- ...



- But Ethereum opened a new chapter in blockchains in 2013.

Ethereum

Ethereum was
proposed by Vitalik
Buterin in 2013~2014.
But it went live in 2015.



The idea of **smart contracts** was first conceived in 1994 by Nick Szabo.
But it was not really realized before Ethereum. Buterin wanted to
generalize the idea of blockchains, and mixed it with programming to
create smart contracts.

Ethereum's Whitepaper

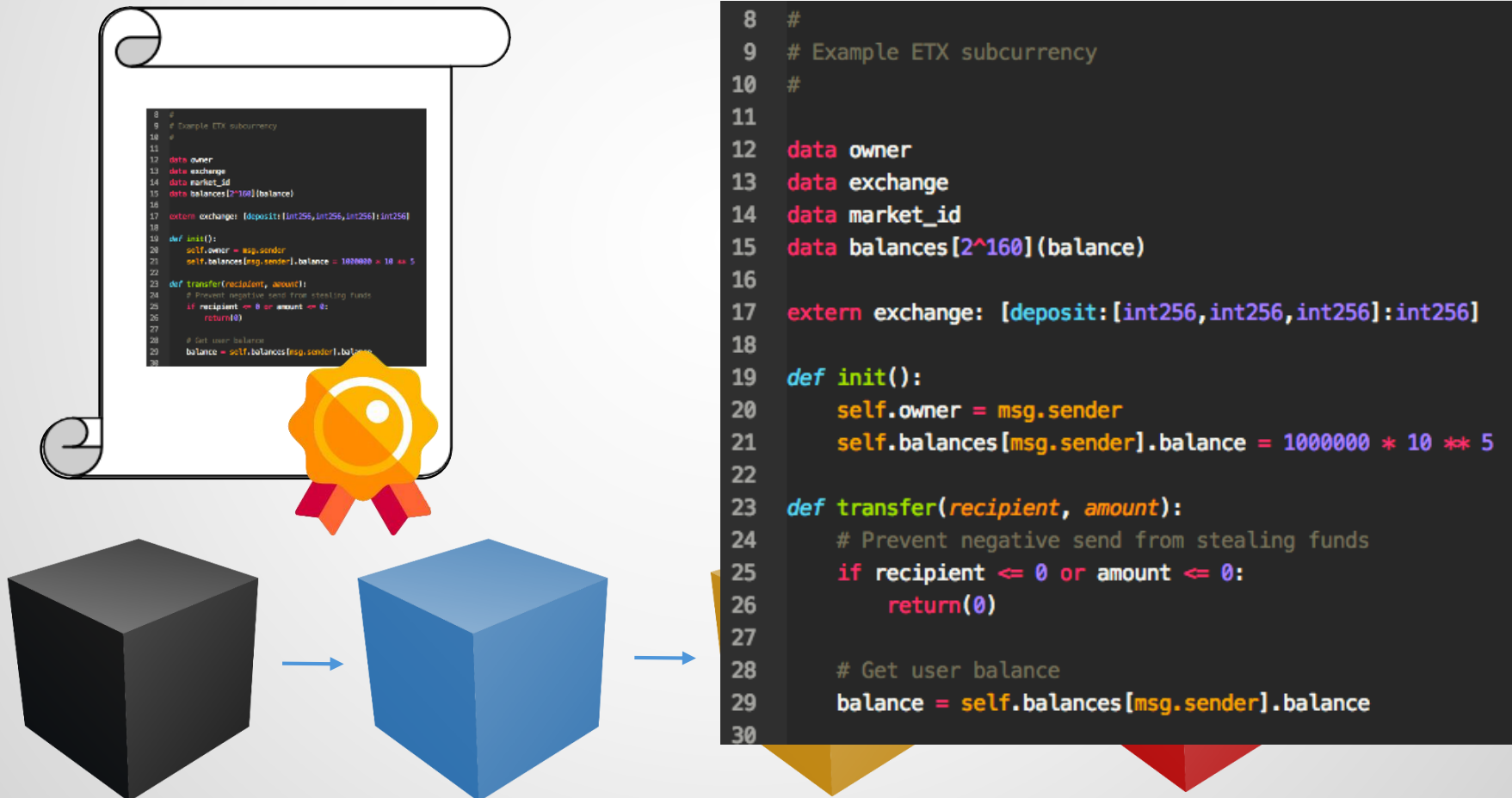


Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.
By Vitalik Buterin (2014).

When Satoshi Nakamoto first set the Bitcoin blockchain into motion in January 2009, he was simultaneously introducing two radical and untested concepts. The first is the "bitcoin", a decentralized peer-to-peer online currency that maintains a value without any backing, intrinsic value or central issuer. So far, the "bitcoin" as a currency unit has taken up the bulk of the public attention, both in terms of the political aspects of a currency without a central bank and its extreme upward and downward volatility in price. However, there is also another, equally important, part to Satoshi's grand experiment: the concept of a proof of work-based blockchain to allow for public agreement on the order of transactions. Bitcoin as an application can be described as a first-to-file system: if one entity has 50 BTC, and simultaneously sends the same 50 BTC to A and to B, only the transaction that gets confirmed first will process. There is no intrinsic way of determining from two transactions which came earlier, and for decades this stymied the development of decentralized

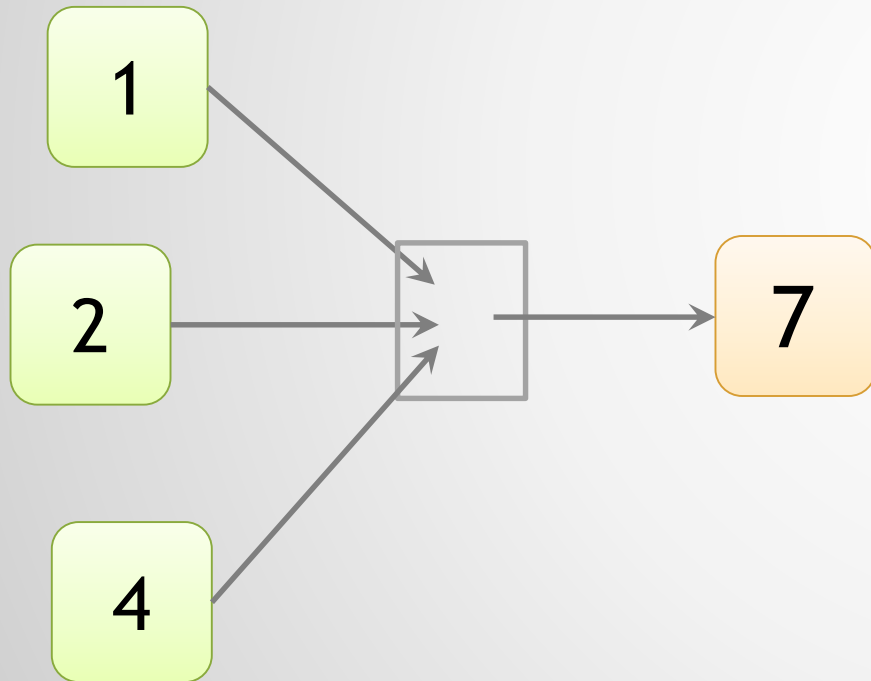
What is a Smart Contract? (animated)

- It's a piece of code or computer program, stored in blockchain.



A Different yet Similar Management

Bitcoin (transaction-based)



Ethereum (account-based)

Address: 0x39ae1..

Balance: 5.2 ETH

Contract/Code:

“

b=b+i;

....

“

It's more efficient to update a balance rather than keeping the track of unspent transactions. It's easier to look up during programming too. However, anybody who wants to verify the correctness of states, must revert to the transactions.

Ethereum Account Types



Externally (user)-owned Accounts

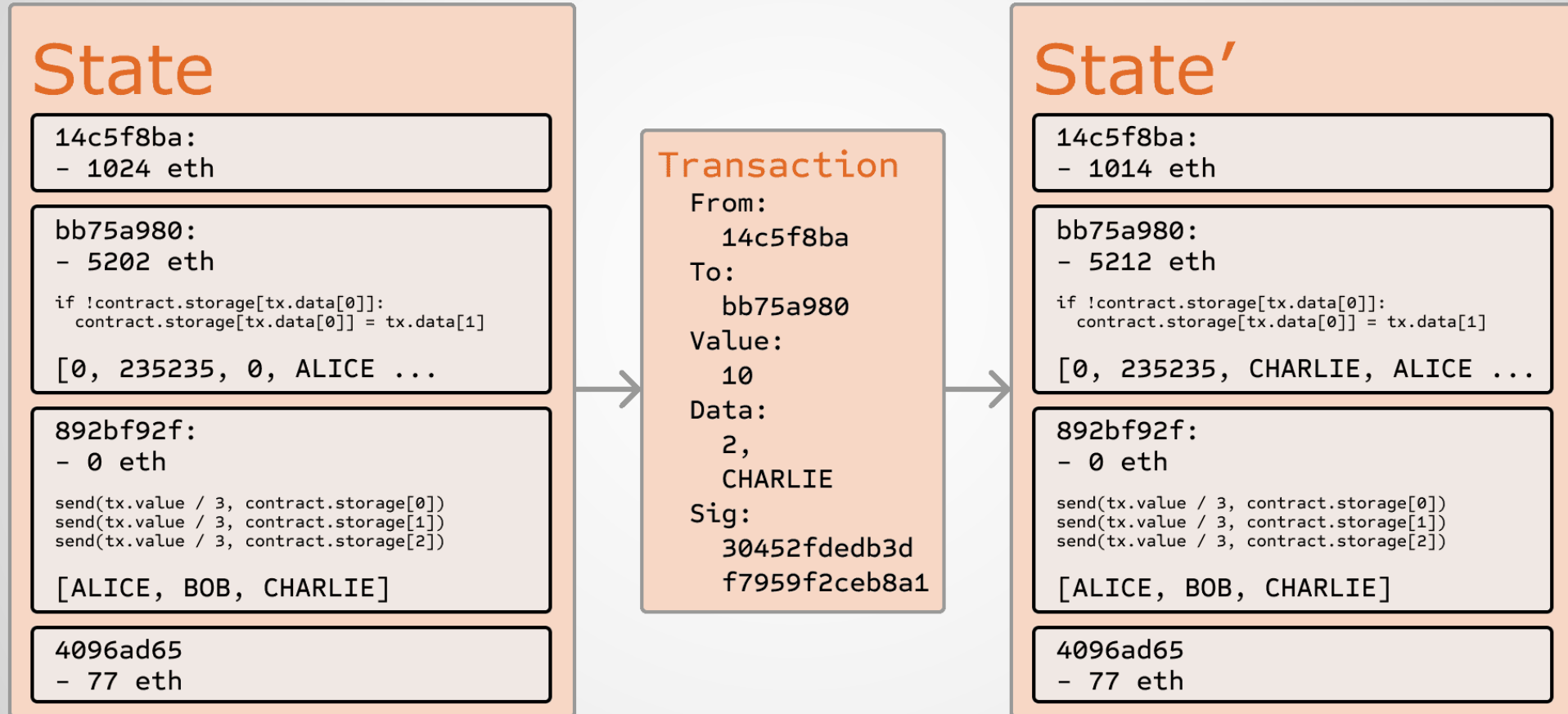
- Owned by an active external body (e.g. person or company)
- Is able to submit transactions (to trigger running of a contract or to transfer money)
- Mainly has: Address + Balance

```
8 #
9 # Example ETX subcurrency
10 #
11
12 data owner
13 data exchange
14 data market_id
15 data balances[2^160](balance)
16
17 extern exchange: [deposit:[int256,int256,int256]:int256]
18
19 def init():
20     self.owner = msg.sender
21     self.balances[msg.sender].balance = 1000000 * 10 ** 5
22
23 def transfer(recipient, amount):
24     # Prevent negative send from stealing funds
25     if recipient <= 0 or amount <= 0:
26         return 0
27
28     # Get user balance
29     balance = self.balances[msg.sender].balance
30
```

Smart Contract Accounts

- Owned and managed by a contract.
- Maintains a state
- Execution is triggered by transactions
- Mainly has: Address + Contract + Storage (can contain Balance)

State of the Network is Updated by Transactions

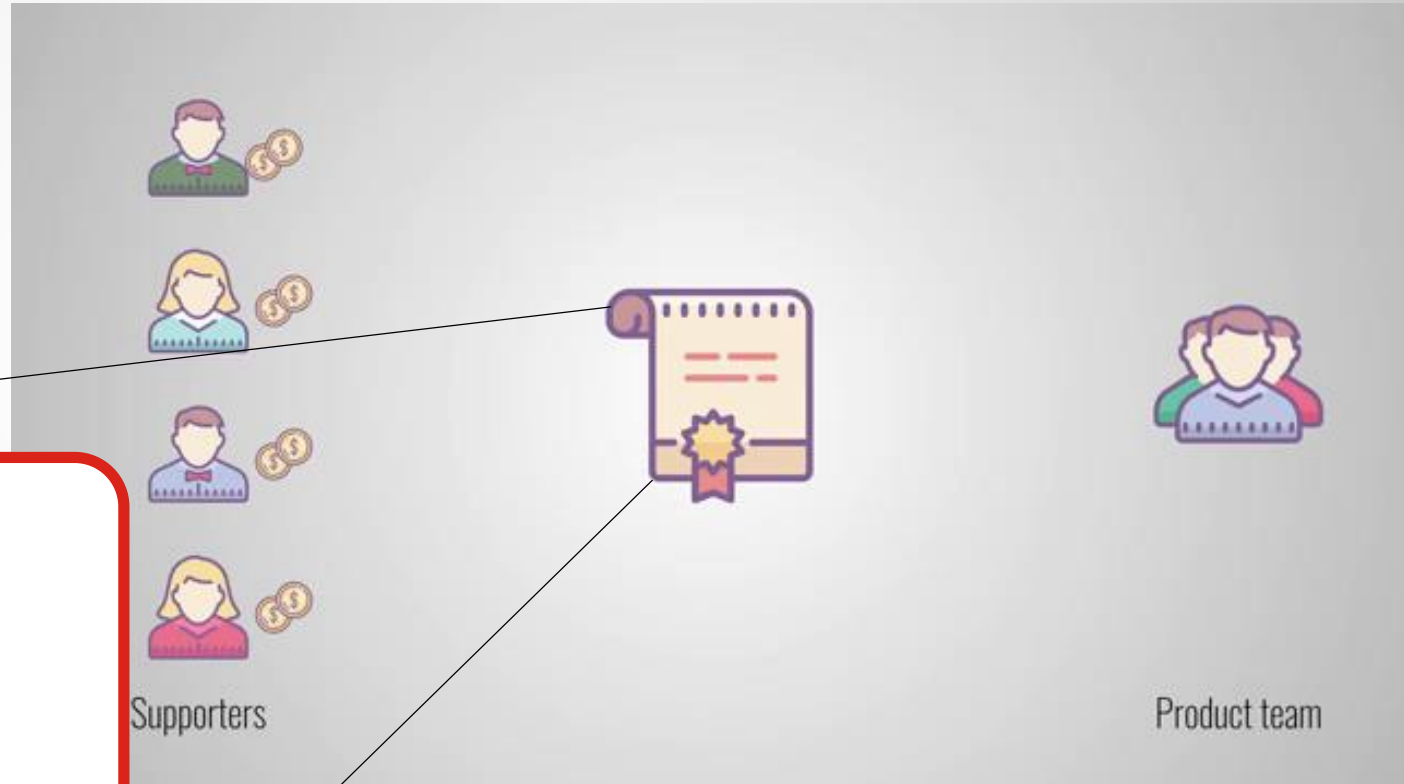


CrowdSourcing with Smart Contracts

In Ethereum, you can interact with smart contracts as well as human beings (2 account types).

You can write a smart contract (program) that collects money for a project.
Programs can have if/then, loops, etc.

```
If the collected money  $\geq T$  , then  
{  
    Transfer money to the team  
}  
else  
{  
    refund the money  
}
```



(Source: Smart Contracts by Savjee)

Blockchain Applications: Auctions and Tenders

➡ Bid history
At the moment, again TTPs are doing auction/tender management.

➡ Auction/Tender is a binding contract.

➡ We can remove TTPs and do the auctions using a smart contract.

The screenshot shows an eBay Australia item bid page for a Lenovo laptop. The page includes a search bar, a category dropdown, and a search button. The item is a Lenovo laptop, and the current bid is AU \$31.00. The page also displays a bid history table and a section for placing a bid.

Search for anything

All Categories Search Advanced

Back to item description

Bid history

Bidders: 5 Bids: 9 Time left: 19 hours 3 mins 13 secs Duration: 3 days

Only actual bids (not automatic bids generated up to a bidder's maximum) are shown. Automatic bids may be placed days or hours before a listing ends. [Learn more about bidding.](#)

Show automatic bids

Bidder	Bid amount	Bid time
0***0 (1)	AU \$31.00	22 Jun 2018 at 19:21:53 AEST
k***a (19 ★)	AU \$30.00	22 Jun 2018 at 16:26:15 AEST
0***0 (1)	AU \$29.00	22 Jun 2018 at 19:21:55 AEST
0***0 (1)	AU \$22.00	22 Jun 2018 at 19:22:00 AEST
3***2 (61 ★)	AU \$25.00	21 Jun 2018 at 12:56:36 AEST
k***a (19 ★)	AU \$25.00	22 Jun 2018 at 16:26:11 AEST
e***t (19 ★)	AU \$20.00	21 Jun 2018 at 10:25:31 AEST
e***t (19 ★)	AU \$5.00	21 Jun 2018 at 10:25:15 AEST
z***z (11 ★)	AU \$1.00	21 Jun 2018 at 1:23:27 AEST
Starting price	AU \$0.99	20 Jun 2018 at 19:00:04 AEST

Current bid: AU \$31.00

Postage: AU \$30.00 Standard Postage

Item number: 123201479622

Enter your maximum bid:

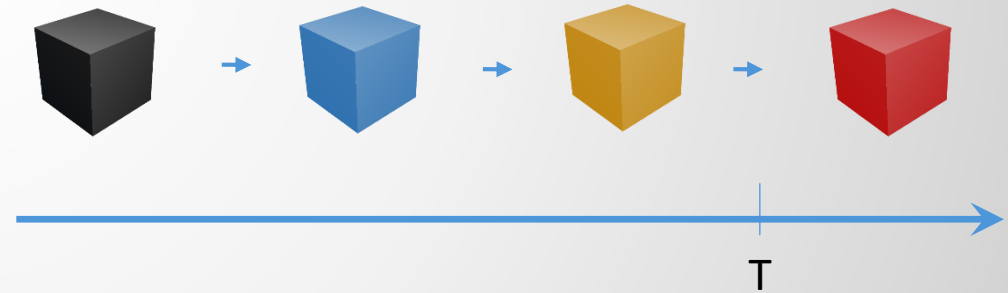
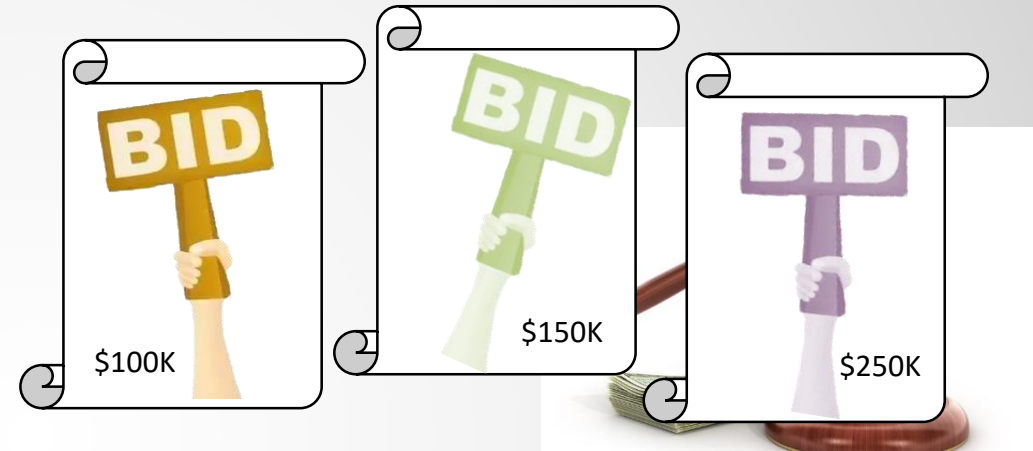
Place bid

(Enter AU \$32.00 or more)

Blockchain Applications: Auctions & Tenders

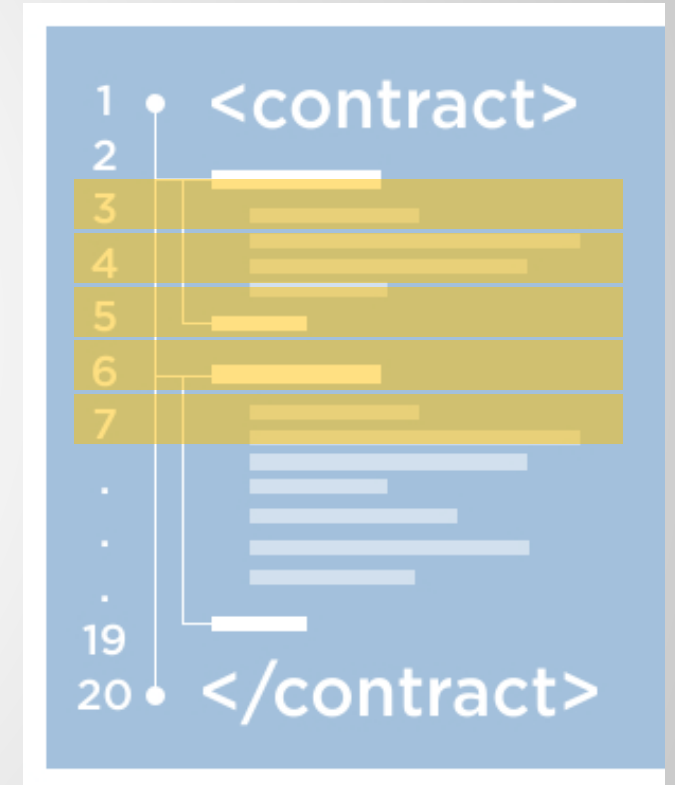
- Transactions to the contract (offers/bids) can be verified by everybody and everything is transparent.

```
If (offer > Greatest_offer & t < T) then
{
    Increase to the highest bid
    Switch to the new buyer
}
else
{
    keep the current bid and buyer
}
```



How is the Consensus Reached on a Contract?

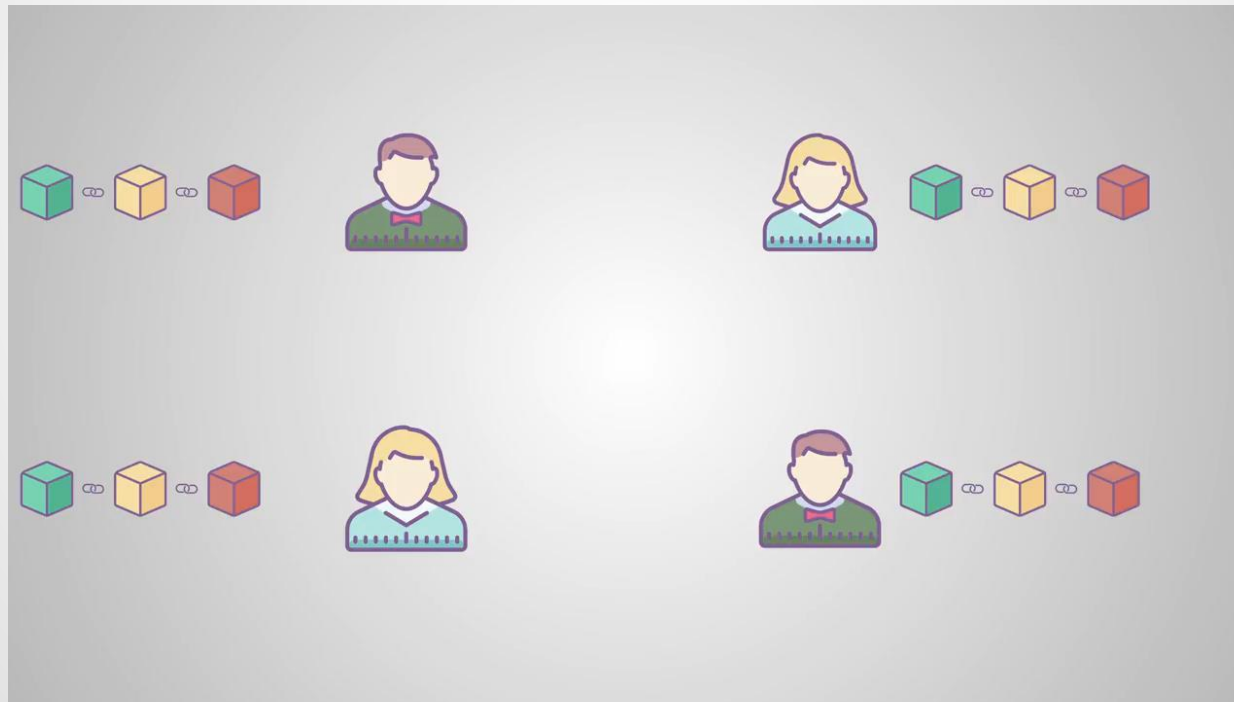
- Similar to Bitcoin, everybody receives a copy of the smart contract (program) as well as all the other interactions done with it.
- Everybody can run the code on their computer and give it the same interactions to find the current state of the contract.



(bitsonblocks.net)

How is the Consensus Reached on a Contract?

- Again, we can use the blockchain to ease the processing and make sure the interactions are in the correct order.



(Source: Smart Contracts by Savjee)

What Comes Next ...

- We learned the core idea behind Ethereum, i.e. smart contracts.
- We saw how complex programs can potentially be implemented on this decentralized platform under zero trust assumption.
- We next learn about Ethereum Virtual Machine and the concept of gas.

