EDU

CSDN学院　IT实战派

以太坊基础

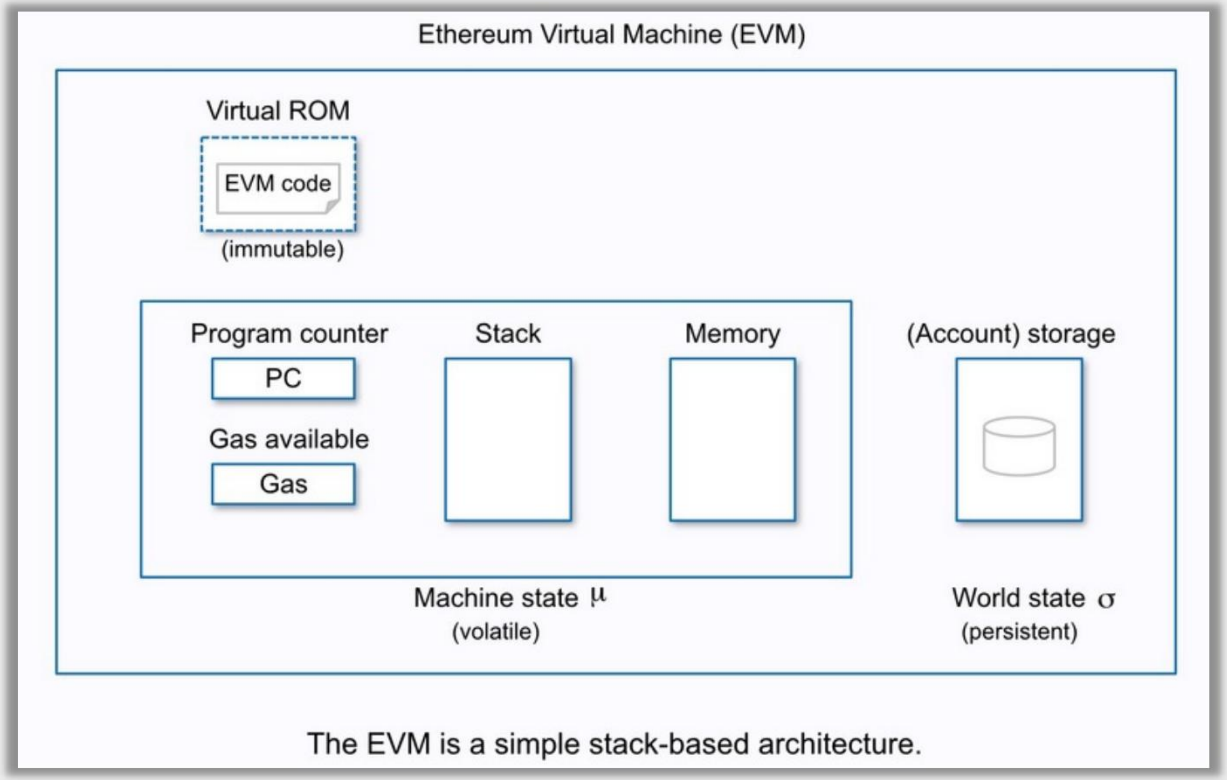
以太坊中的基础概念

讲师：康烁

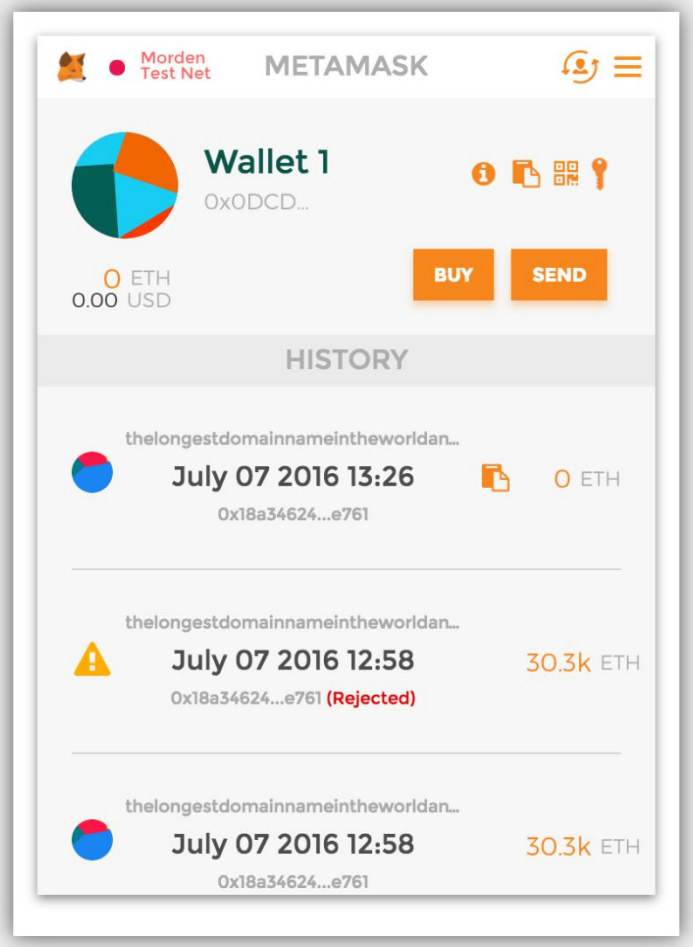
本节目标

1. 理解以太坊虚拟机
2. 理解以太坊的账号和交易

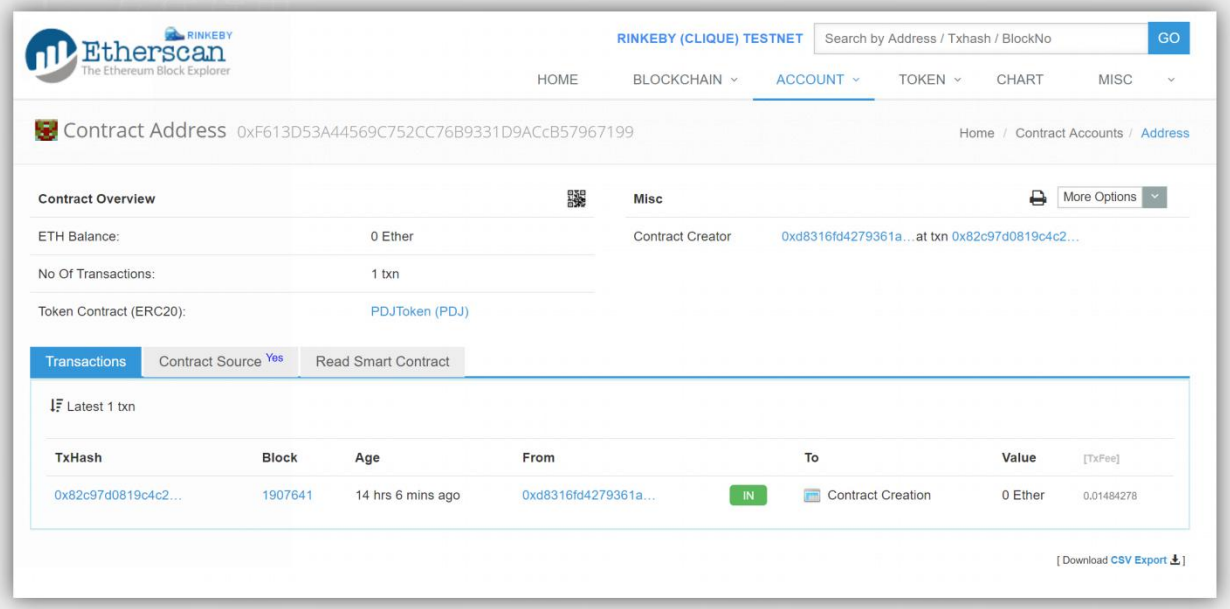
以太坊虚拟机



以太坊的帐户

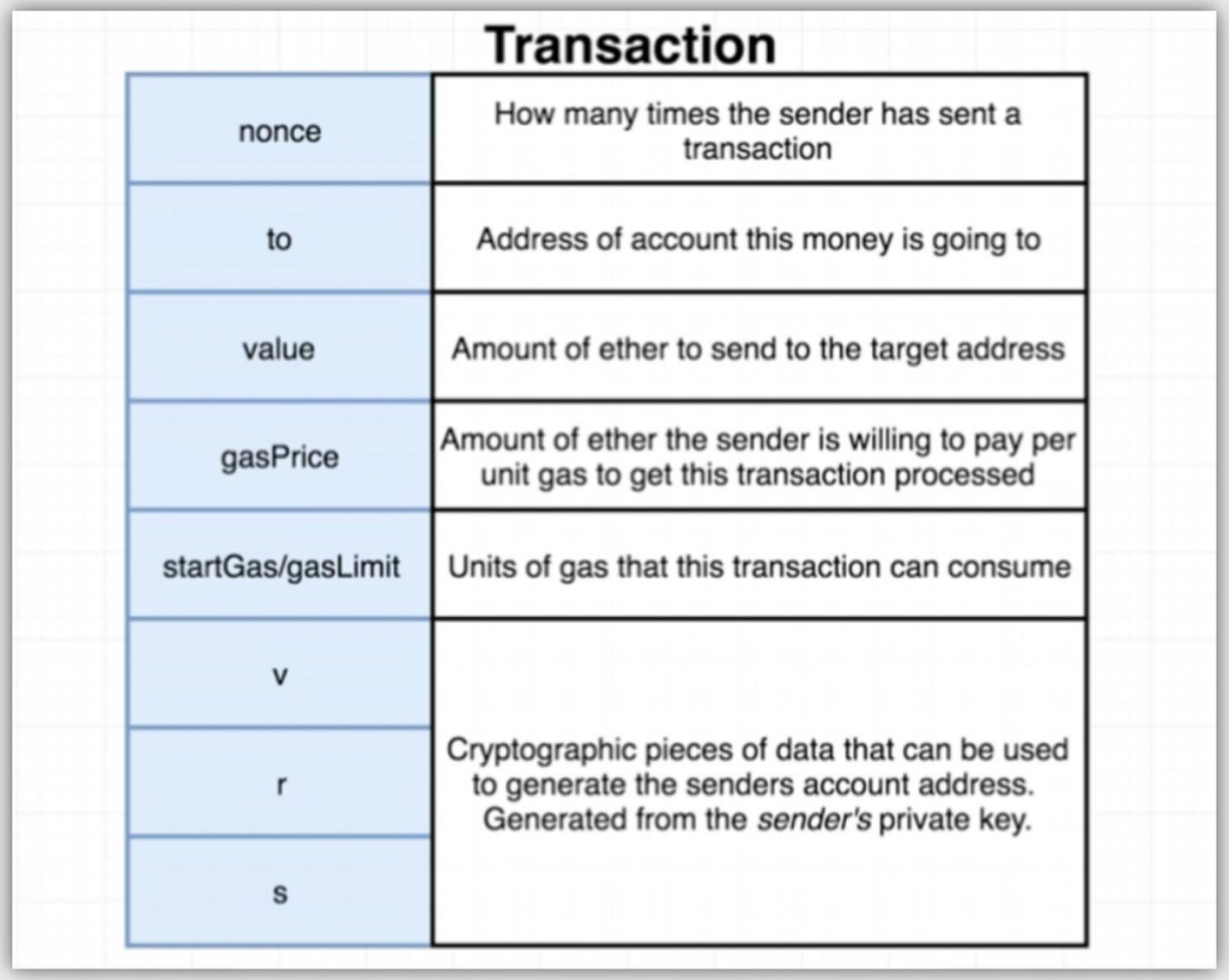


1. 外部所有者帐户
2. 智能合约帐户



以太坊的交易

1. 交易是以太坊里的基本操作
2. 以太坊的交易有两个基本类型，一种是汇款交易，一种是智能合约调用交易

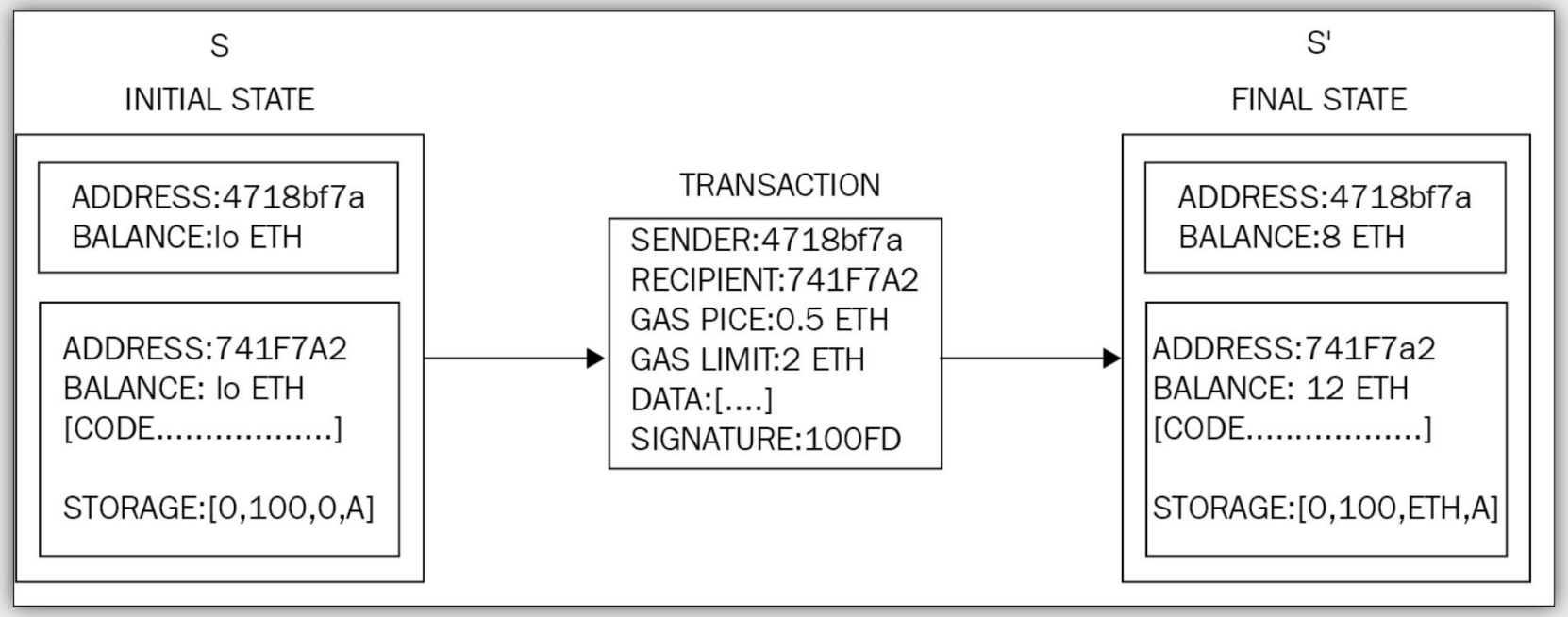


以太坊相对于比特币的几处改动

1. 挖矿：Ethash/Keccak 哈希算法，防止 ASIC 加速
2. 更短的出块时间（14-15秒）
3. 对叔块（Uncle/Ommer block）予以奖励
4. 基于账户的模型（EOA 账户和合约账户）
5. 智能合约和 EVM
6. Gas、Gas Price、以太币和经济系统
7. 社区治理

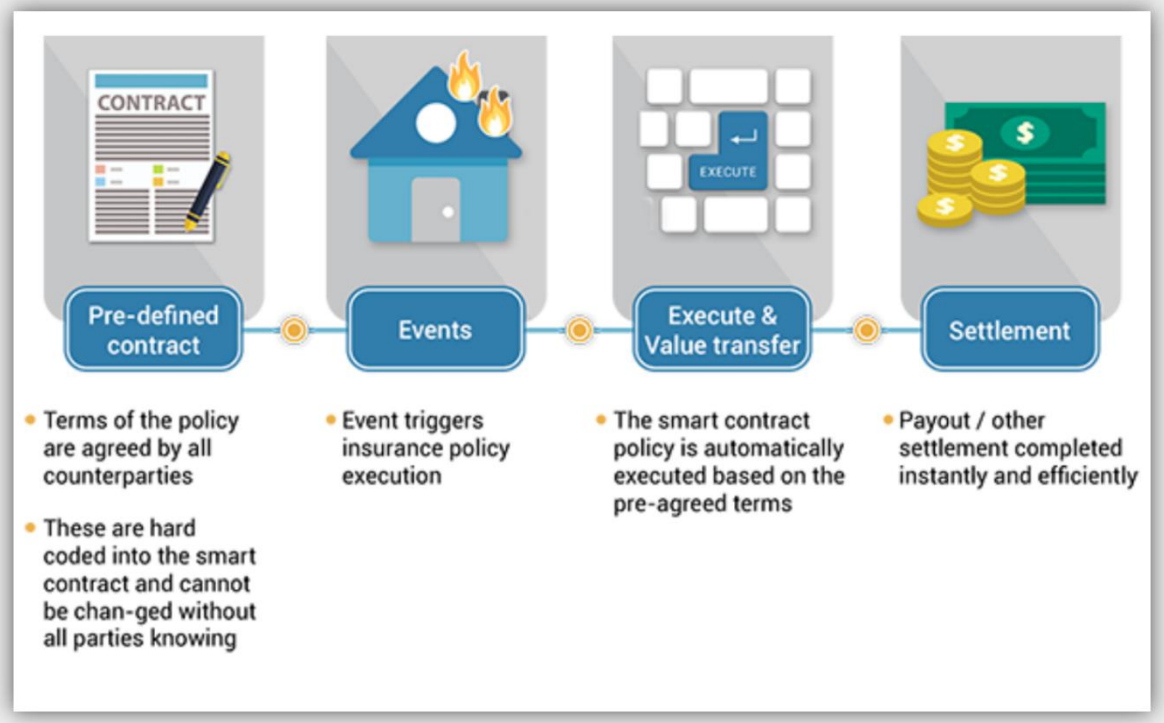
状态

以太坊要实现一个全球计算机，除了要有统一的 CPU 之外，各节点还需要有一致的内存和硬盘数据状态。我们将内存和硬盘数据状态视为一体，在以太坊中被统称为状态（“state”）



事件

- 在合约执行当中，可以发布事件。其他合约可以检测事件，从而可以作出相应的动作
  - 举例：如果有一个智能合约专门负责收款，另一个智能合约负责分钱，那么当收款的智能合约收到款的时候，它可以发送一个事件，说“已经收到款了”，而负责分钱的智能合约监听到这个事件之后，就会执行分钱的操作，按照事先的约定，把款项分给相应的 EOA



消息

一个合约可以向另一个合约发送消息（messages），消息是 EVM 环境内的虚拟对象，不会被序列化或者保存起来。消息其实跟交易是非常相似的，只不过交易是由 EOA 发起的，而消息则是由一个合约发给另一个合约的

msg.sender: 发起交易的账户

msg.receiver: 接受交易的账户

msg.value: 随着该消息发送的汇款的数量，以 wei 为单位 (1 wei = 10E-18 ETH)

msg.data: 一个可选字段，其中包括输入数据。汇款交易没有输入数据，所以这个字段为空。

msg.startgas: 限定了由这个 msg 触发的运算所能消耗的 Gas 上限

以太坊交易处理的完整过程

1. 新的交易提交给一个节点，该节点首先验证交易是否合法，如不合法则拒绝
2. 合法交易向全网广播，接收到的矿工节点首先将交易放入交易池中候选
3. 矿工节点选择本回合打包的交易，并验证交易是否合法
   - 检查交易签名
   - 检查交易发送者合法
   - 检查交易的 nonce 值与交易发送者账户中的 nonce 值是否一致
   - 确认本交易的 gas limit 大于交易静态 gas 消耗
   - 如果是支付操作，确认汇款方账户余额充足
   - 确认本交易消耗的 gas 不会突破整个区块的 gas limit
4. 执行每一个智能合约，实施状态变迁
5. 矿工节点检查六代之内的叔块（uncles/ommers）
6. 将叔块矿工应得的奖励写入下一个区块（Applying ）
7. 寻找 Nonce 值，一旦找到立刻向全网广播新区块；若没有找到 Nonce 值，而是收到了别的节点获胜的消息，那么就迅速对比获胜节点发来的区块、交易池和自己正在打包的交易，剔除掉已经被别人打包的交易，选取新的一组交易，马上开始下一轮挖矿、打包的竞赛。

以太坊的最大问题：性能

交易速度：

比特币 ： 4TPS

以太坊 ： 13TPS

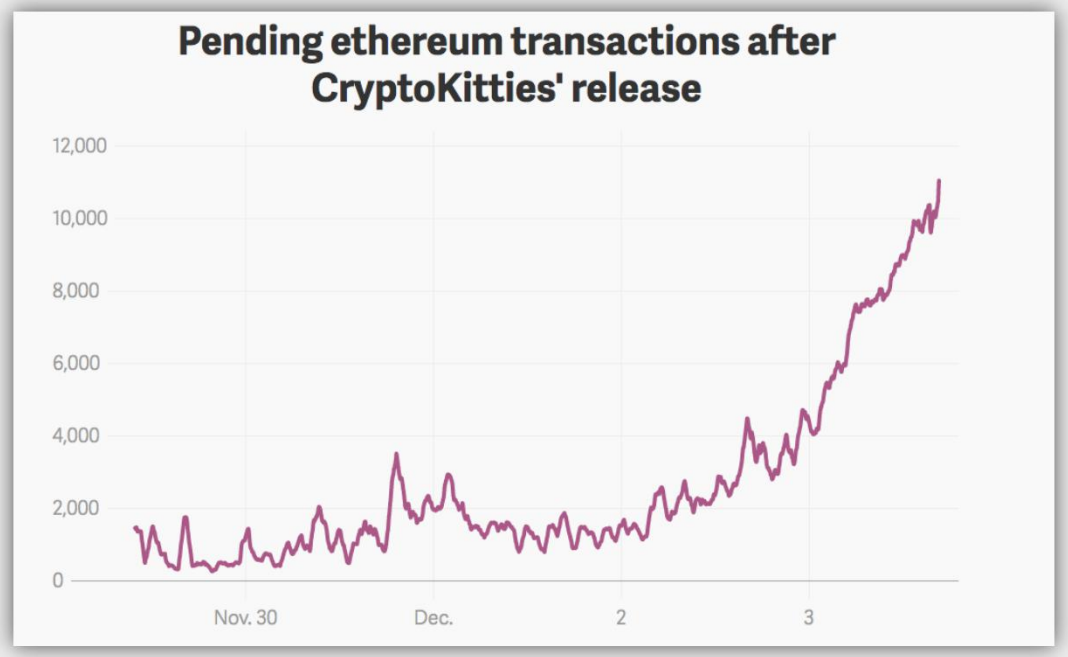
VISA ： 2000TPS

延迟：

比特币30分钟，

以太坊一分钟左右；

加密猫阻塞以太坊



https://qz.com/1145833/cryptokitties-is-causing-ethereum-network-congestion

https://etherscan.io/chart/tx

总结

1. 以太坊的虚拟机
2. 以太坊的交易和事件

布置作业

- 必做内容：
- 理解以太坊的账号和交易
- 理解以太坊的事件

EDU

CSDN学院　IT实战派