北京大学
PEKING UNIVERSITY

区块链课程

孙惠平
sunhp@ss.pku.edu.cn

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

北京大学
PEKING UNIVERSITY

PART 第四章

以太坊

目 录

CONTENTS

第1节

以太坊概述

01 以太坊的概念

02 以太坊与比特币的比较

03 以太坊的发展历史

04 以太坊的关键组件

05 以太坊的应用

01 以太坊的概念

- 我们可以用一句话概括以太坊：

定义

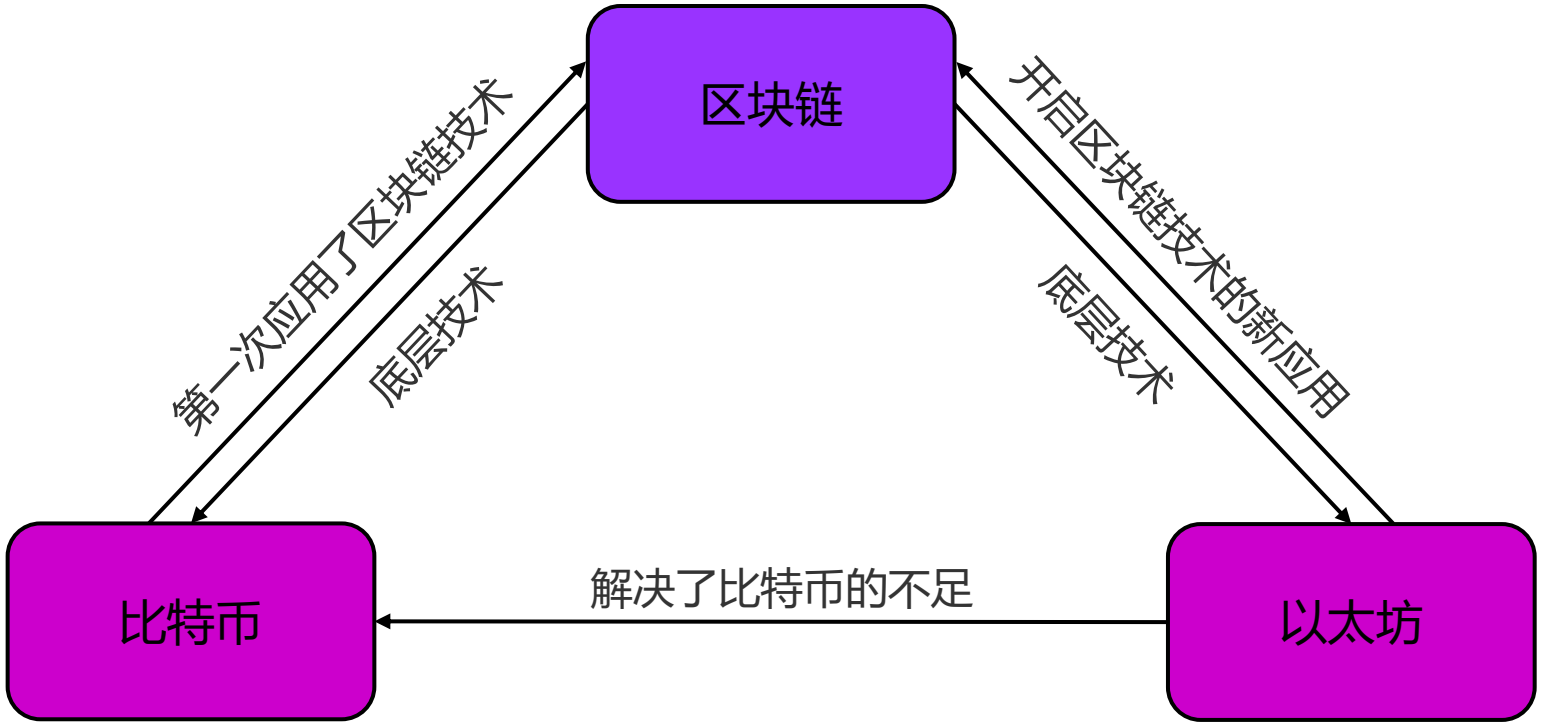
以太坊（Ethereum）是一个基于**区块链**的**智能合约**平台。

区块链是一种新型去中心化协议，能安全地存储交易或其它数据。“区块链”的概念来源于比特币，它最大的好处是链上信息不能被用户伪造和篡改，无需任何中心化机构的审核。

智能合约是一种在区块链上运行的计算机程序，这段计算机程序是预先设计好的一套数字化规则，它包含真实世界经多方协商达成一致的业务逻辑。

02 以太坊与比特币的比较

- 您已经在上一章学习过了比特币的概念，可以用下图来描述以太坊和比特币之间的联系和区别：



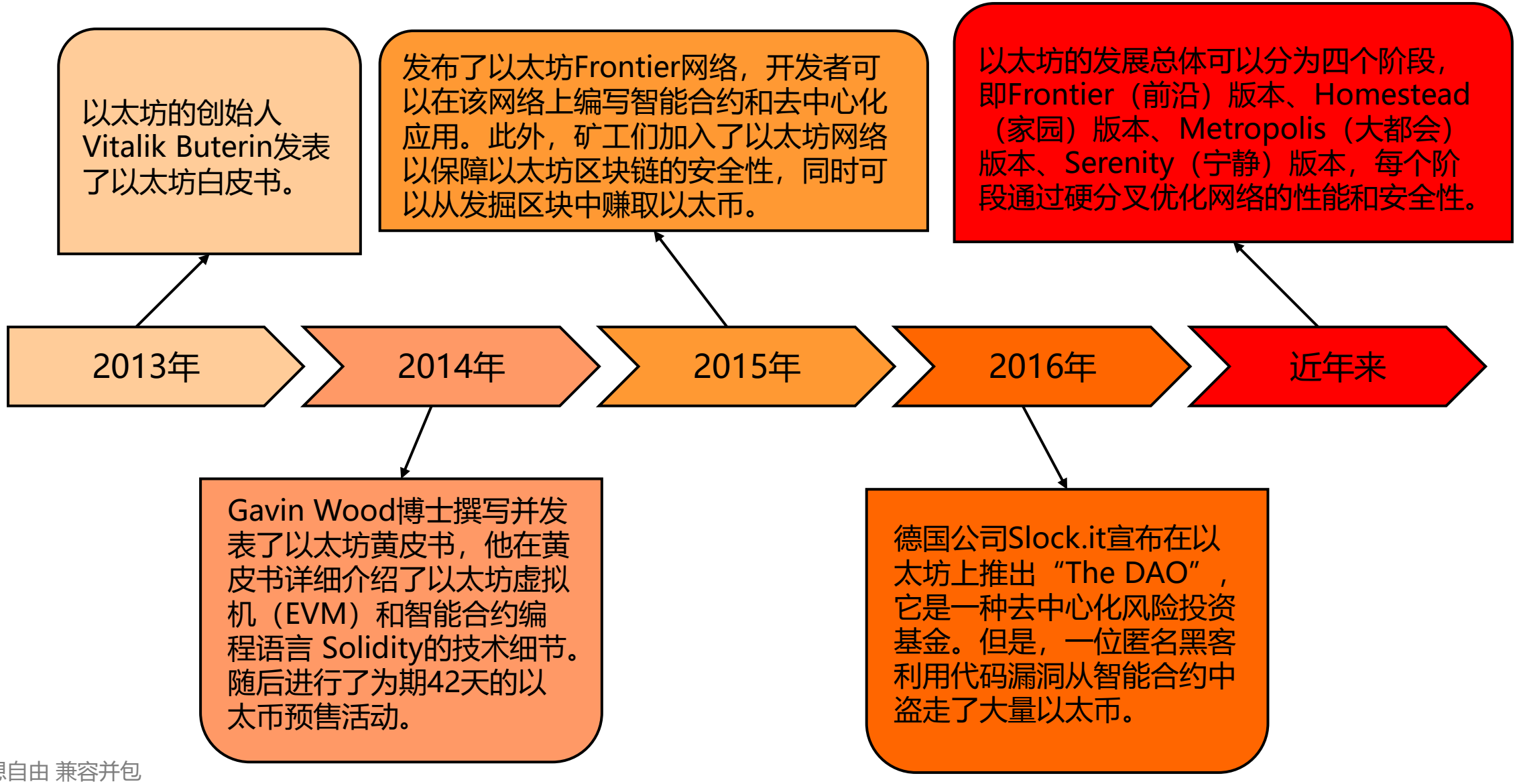
02 以太坊与比特币的比较

- 可以说，以太坊是区块链的新生代应用。根据应用的范围不同，人们通常把区块链技术的发展阶段概括为三个时代：

区块链1.0 → 区块链2.0 → 区块链3.0 → …

区块链1.0	区块链2.0	区块链3.0
关键词 比特币	**关键词** 以太坊	**关键词** ？
概述 比特币是对区块链技术的**第一个应用**，它充分验证了区块链技术的可行性和安全性，而且实现了**去中心化的数字货币支付功能**。但是，比特币也存在功能单一、涉及行业较少的缺点。	**概述** 以太坊开启了区块链技术应用的新世界，它的核心是**智能合约**，并且提供了多种工具让用户在其平台上搭建应用。智能合约将各行业紧密联系起来，使区块链技术有了更加广泛的应用。	**概述** 未来数年内，区块链技术将在很多领域有更深入的应用，包括：物联网、金融交易、网络安全、公共记录等，它能够显著上述行业的服务流程，甚至颠覆了它们的传统运营模式。

03 以太坊的发展历史


以太坊的创始人Vitalik Buterin发表了以太坊白皮书。
发布了以太坊Frontier网络，开发者可以在该网络上编写智能合约和去中心化应用。此外，矿工们加入了以太坊网络以保障以太坊区块链的安全性，同时可以从发掘区块中赚取以太币。
以太坊的发展总体可以分为四个阶段，即Frontier（前沿）版本、Homestead（家园）版本、Metropolis（大都会）版本、Serenity（宁静）版本，每个阶段通过硬分叉优化网络的性能和安全性。
2013年
2014年
2015年
2016年
近年来
Gavin Wood博士撰写并发表了以太坊黄皮书，他在黄皮书详细介绍了以太坊虚拟机（EVM）和智能合约编程语言 Solidity的技术细节。随后进行了为期42天的以太币预售活动。
德国公司Slock.it宣布在以太坊上推出“The DAO”，它是一种去中心化风险投资基金。但是，一位匿名黑客利用代码漏洞从智能合约中盗走了大量以太币。

04 以太坊的关键组件

北京大学 PEKING UNIVERSITY

- 每个公共区块链都包含若干组件，下面分析以太坊的关键组件：

P2P网络

以太坊运行在以太坊主网络上，这是一个通过TCP 30303端口寻址的网络。

共识机制

以太坊的发展可以分为四个阶段，前三个阶段采用了PoW共识机制，第四个阶段采用了以太坊创建的PoS机制，名称是Casper投注共识。

交易

以太坊交易是一个网络消息，主要包含交易发送者、交易接收者、转移的金额和数据。

状态机

以太坊的状态转换由以太坊虚拟机处理，这是一个基于栈的虚拟机，它可以用来执行字节码。其中，以太坊中的智能合约通常采用高级语言来编写，它们会被编译在以太坊虚拟机中执行的字节码。

数据结构

以太坊的区块链通常采用Google的LevelDB数据库的方式保存在每一个节点之上，区块链内包含了交易和系统的状态，经过哈希处理的数据保存在Merkle-Patricia树结构中。

客户端

以太坊有多个可以供用户与以太坊网络交互的客户端，使用最广泛的是Go-Ethereum和Parity。

05 以太坊的应用

- 用户可以通过以太坊开发去中心化应用（DApp），它在很多领域都有广泛的应用，包括：金融行业、博彩行业、游戏行业、公共事业、供应链、物联网、政府、企业等。例如：

游戏行业

在传统游戏中，玩家购买的游戏装备、游戏道具，表面上是玩家拥有的财产，但实际上玩家仅仅拥有它们的使用权。但是，以太坊的诞生使基于区块链的游戏成为了可能，通常把它们称作“链游”。在链游中，玩家可以边玩游戏边赚钱，同时游戏中资产归属的问题也与传统游戏完全不同。

数字城市

在个人信息中心化的情况下，个人隐私很难被保护，“数字城市”对用户的虚拟画像可能比物理世界更具体。如果基于以太坊实现“数字城市”，那么每个人都可以在其中拥有虚拟的身份，在不泄露个人隐私信息的前提下，各行业对用户的需求预测仍然可以通过隐私计算、AI算法、加密分析完成。

05 以太坊的应用

预测市场

预测市场技术为市场交易人员提供了一种用于预测某一事件二元结果的技术。例如，PredictIt就是一款最受欢迎的预测市场平台软件。这类应用能够把从现实世界获得的信息可信地放入区块链中，因此它们会成为区块链技术的重要应用，它们。如果这项技术变得更加成熟，我们将能够看到一种新的集体智慧管理类型。

社交网络

在以太坊中，有的项目团队正在利用一种评级系统来实现一种去中心化的社交网络，它由智能合约来规范社交行为。这种基于去中心化的社交网络将在未来的生活中扮演重要的角色。

第 2 节

以太坊账户

01 以太坊的地址

02 以太坊的账户及分类

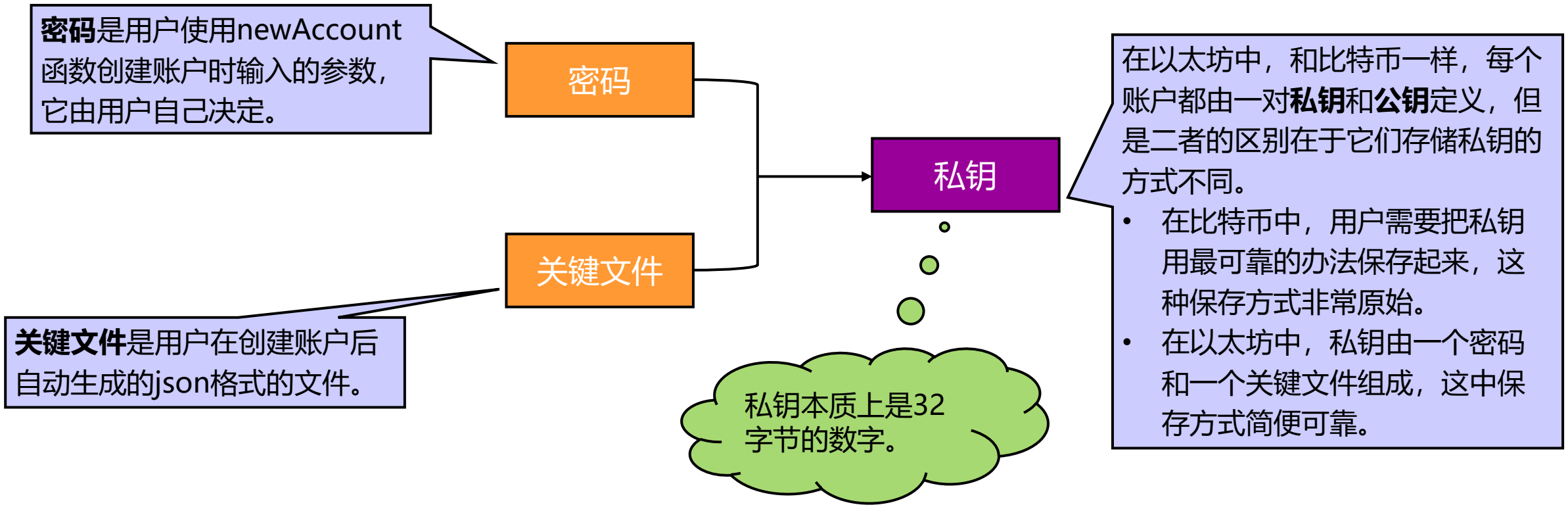
03 以太坊的钱包

04 以太币

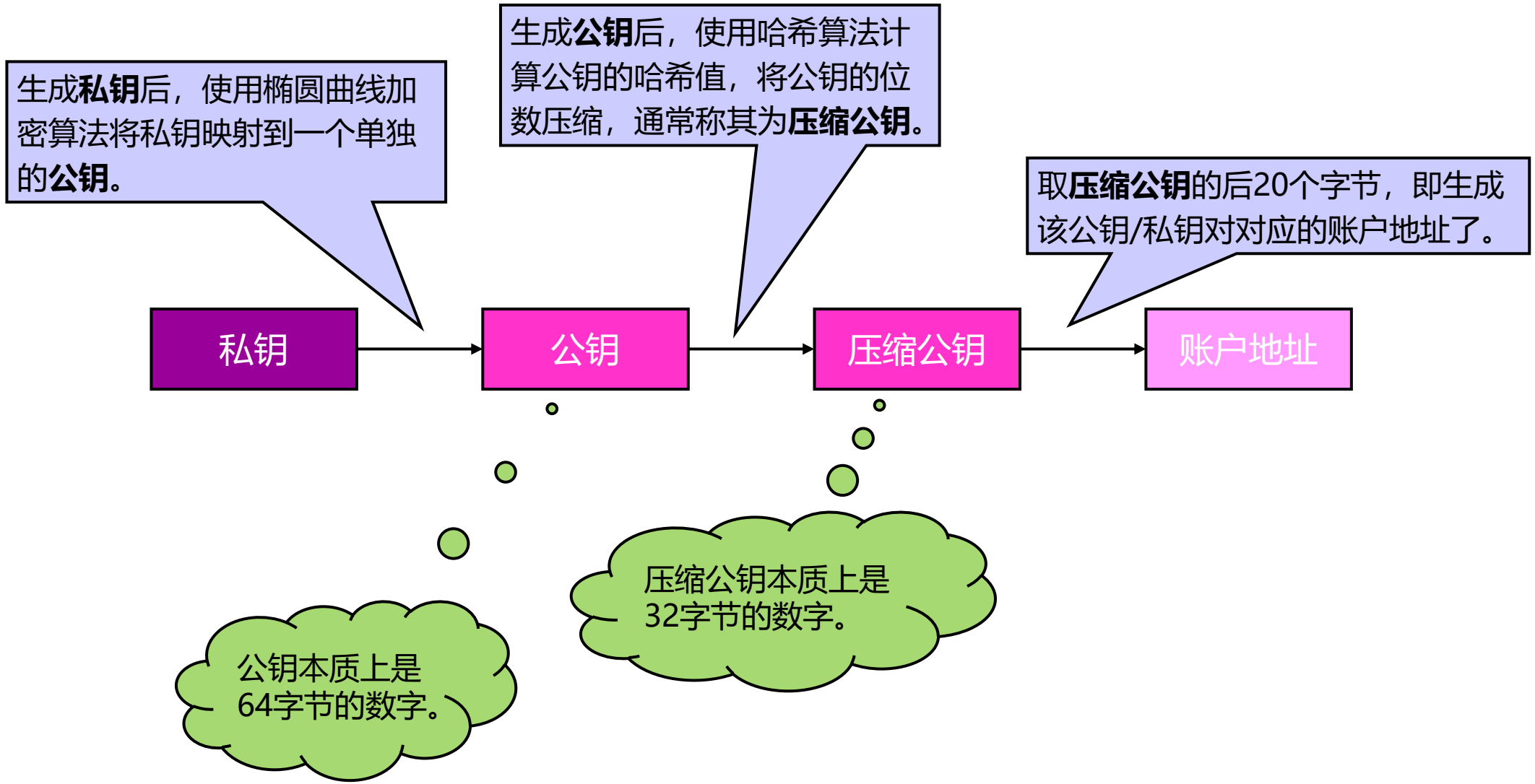
05 gas

01 以太坊的地址

- 和比特币类似，以太坊也存在公钥、私钥和地址的概念，它们的关系是这样的：



01 以太坊的地址


生成**私钥**后，使用椭圆曲线加密算法将私钥映射到一个单独的**公钥**。
生成**公钥**后，使用哈希算法计算公钥的哈希值，将公钥的位数压缩，通常称其为**压缩公钥**。
取**压缩公钥**的后20个字节，即生成该公钥/私钥对对应的账户地址了。
私钥
公钥
压缩公钥
账户地址
公钥本质上是64字节的数字。
压缩公钥本质上是32字节的数字。

02 以太坊的账户及分类

和人们平常接触到的银行账户一样，以太坊中的账户是用户进行交易的标识。当进行一笔交易时，需要明确以太币的支出账户和接收账户。但是，与普通银行账户不同的是，以太坊账户具有良好的匿名性，这体现在以下几个方面：

- 普通银行账户需要在银行实名登记，而以太坊账户的数据不会被记录到系统的数据库中；
- 账户的创建者不需要公布他名下的账户，这体现了区块链的匿名性；
- 由于创建账户仅需要一个自定义的字符串和生成的关键文件，因此用户可以在离线状态下创建账户。

02 以太坊的账户及分类

- 以太坊账户可以分为两种：**合约账户**和**外部账户**。

如果以太坊只有外部账户的话，那它的功能跟比特币就没什么区别了。

外部账户

外部账户是由用户创建的账户，通过公钥/私钥对产生地址，该地址对应唯一的外部账户。用户在使用外部账户交易时，交易信息会被账户对应的私钥签名，这样系统可以安全地认证交易发送者的身份。用户可以随意创建外部账户，在创建外部账户时不需要支付任何费用，外部账户之间的交易也不消耗费用。

合约账户

合约账户是由外部账户创建的账户，创建合约账户时需要消耗一定的以太币。每个合约账户对应唯一的合约代码，合约账户只受到合约中代码控制。它可以暂存以太币，在合适的条件下将可以其发送给其他账户。合约账户的代码需要其他账户发送交易来触发执行，每次执行时需要消耗一定的以太币。合约账户拥有属于自己的存储空间，每次执行代码后变量的状态都会存储在区块链上。

02 以太坊的账户及分类

- 下面总结一下**合约账户**和**外部账户**的区别：

	外部账户	合约账户
账户控制者	用户	合约代码
是否拥有以太币	是	是
是否包含代码	否	是
是否可以发送交易	可以主动发送以太币交易，也可以发送触发代码执行的交易	不能主动发送交易；当合约代码被触发执行时，可以被动向其他账户发送交易
创建时是否消耗以太币	否	是
发送交易时是否消耗以太币	发送以太币交易时不消耗，发送触发代码执行的交易时需要	是

03 以太坊的钱包

- 由于每个用户可以创建多个以太坊账户，因此当用户想管理以太坊账户时，就需要用到以太坊钱包。这就类似于用户在移动支付平台上绑定了多张银行卡时，需要一个管理银行卡的功能。通常情况下，有以下几种钱包供用户选择：

钱包分类	安全性	实用性	实现方式	代表钱包
手机钱包	中等	高	手机钱包允许用户在任何地方访问账户	imToken
浏览器钱包	中等	高	浏览器钱包允许用户在浏览器与帐户交互	MetaMask
物理硬件钱包	高	一般	物理硬件钱包是能够线下保存加密资产的设备	Ledger
桌面钱包	中等	高	桌面钱包允许用户在MacOS、Windows等系统上管理账户	Jaxx

04 以太币

- 以太币是类似于比特币的一种加密货币，它在以太坊系统中流通，用于维护以太坊网络健康可持续运行。以太币有以下两个功能：

交易的媒介

以太币作为一种数字资产在以太坊账户之间流通，它是账户之间交易的主要媒介。

支付矿工的费用

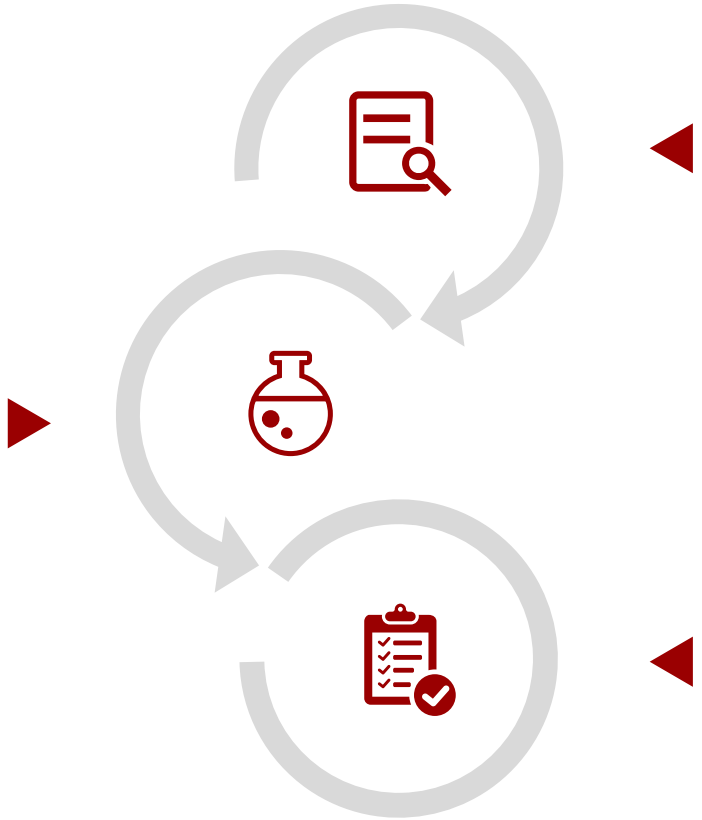
与比特币的挖矿原理相似，以太坊需要通过一种激励机制吸引全世界的矿工加入，该激励机制即奖励矿工一定数量的以太币，矿工可以为以太坊中发生的所有交易提供打包服务。

04 以太币

- 早期以太币可以通过比特币购买。可以说，以太币的发行与比特币密不可分。

以太币的产出

以太坊上线后，矿工每挖到一个区块会获得5个以太币的报酬。有些矿工虽然也挖到区块，但他们的区块因为网络原因没有被添加到区块链上，此时他们仍然会获得2~3个以太币的报酬。根据预售时各方商定的结果，每年以太币发行的上限是1800万。



以太币的预售活动

2014年，在主网上线之前，以太坊展开了以太币预售活动。在预售期的前两周，用户可以用1个比特币购买2000个以太币，随着时间的推移，这个汇率降低到了1个比特币购买1337个以太币。

预售活动的募集资金

预售活动总计募集了大约6000万以太币，其中1200万以太币用作以太坊开发资金，其余大部分分配给了以太坊的早期开发者。

04 以太币

- 以太币的单位最基础的单位是wei，它是用虚拟币先驱人物——戴伟（Wei Dai ）命名的。Wei是一个很小的单位，常用的以太币单位换算如下表：

单位	wei值	别名
wei	1 wei	
Kwei	1×10^{3} wei	Babbage
Mwei	1×10^{6} wei	Lovelace
Gwei	1×10^{9} wei	Shannon
microEther	1×10^{12} wei	Szabo
milliEther	1×10^{15} wei	Finney
Ether	1×10^{18} wei	

- gas是以太坊内部一种特殊的费用计量单位。

产生原因

以太坊在执行每次操作的时候都会消耗一定的资源，例如计算资源、存储资源等，因此用户若想使用以太坊的资源，就需要向网络中的矿工支付一定的费用。由于计算机执行每次任务消耗的资源量几乎是恒定的，用户也希望自己支出的费用不会因为以太币价格的波动而有太大的变化。因此，需要制定一种以太坊内部的费用计量单位。

定义

gas是用来衡量交易耗费的计算资源的一种计量单位。

特性

不可交易性

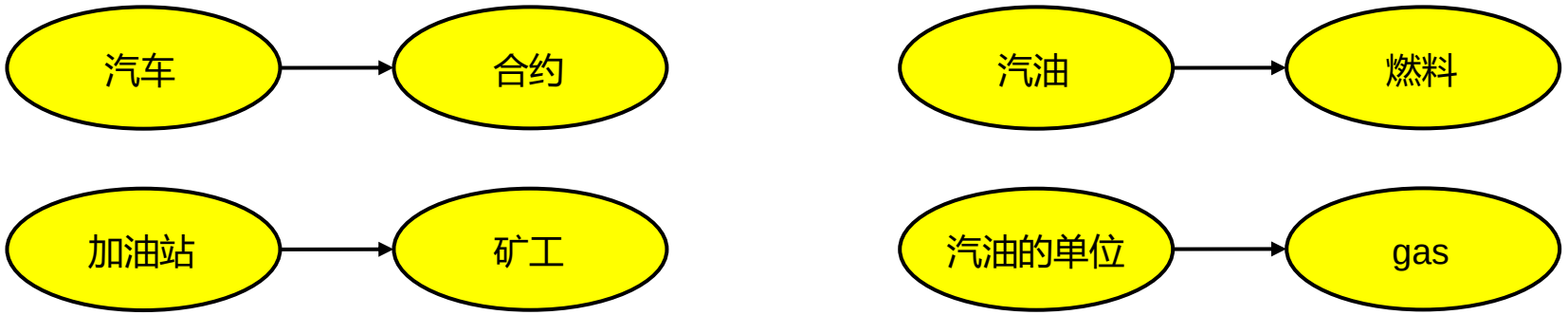
gas只是一种衡量耗费资源的单位，因此它不能在以太坊中交易，矿工需要将gas转换成以太币作为收益。

价值恒定性

在gas兑换成以太币的过程中，以太坊通过一系列机制保证gas的价值不会发生太大变化。

解读

gas可以理解为驱动以太坊运行的“燃料”，以太坊中的一切交易都要消耗一定量的gas。例如在现实生活中，如果想让汽车一直运转，那么汽油就是驱动汽车运转的燃料，那么就需要定时去加油站加油。在这个例子中，汽车扮演合约的角色，加油站扮演矿工的角色，汽油扮演燃料的角色，而汽油的计量单位就是gas。



05 gas

- 以下是与gas相关的几个概念：

gas

gasPrice

gasPrice表示用户愿意支付每单位gas的价格，即每单位gas可以兑换的以太币数量。为了保证每单位gas价值的稳定，gasPrice会根据市场的波动而变化，市场会保持用户愿意支付的价格与矿工能够接受的价格处于平衡的范围。也就是说，矿工会优先打包gasPrice高的交易。

gasCost

gasCost表示以太坊节点在执行某种操作时花费的gas数量，它的值一般是恒定的，这表明每种操作所花费的成本几乎不会发生变化。

gasLimit

gasLimit表示用户愿意为一笔交易花费的最高gas数量，当实际消耗的gas达到gasLimit的值的时候，交易就会终止。也就是说， gasLimit给一笔交易能够消耗的gas数量设定了一个上限。一个标准的发送以太币的交易所设定的gasLimit一般是21000。

gasFee

gasFee表示实际执行一笔交易的过程中实际需要支付的gas数量。一个区块的gasFee可以用来推测出该区块消耗的计算量、所包含交易的数量以及一个区块的大小。gasFee最终都会支付给矿工。

第 3 节

以太坊架构

01 以太坊架构的概述

02 服务层

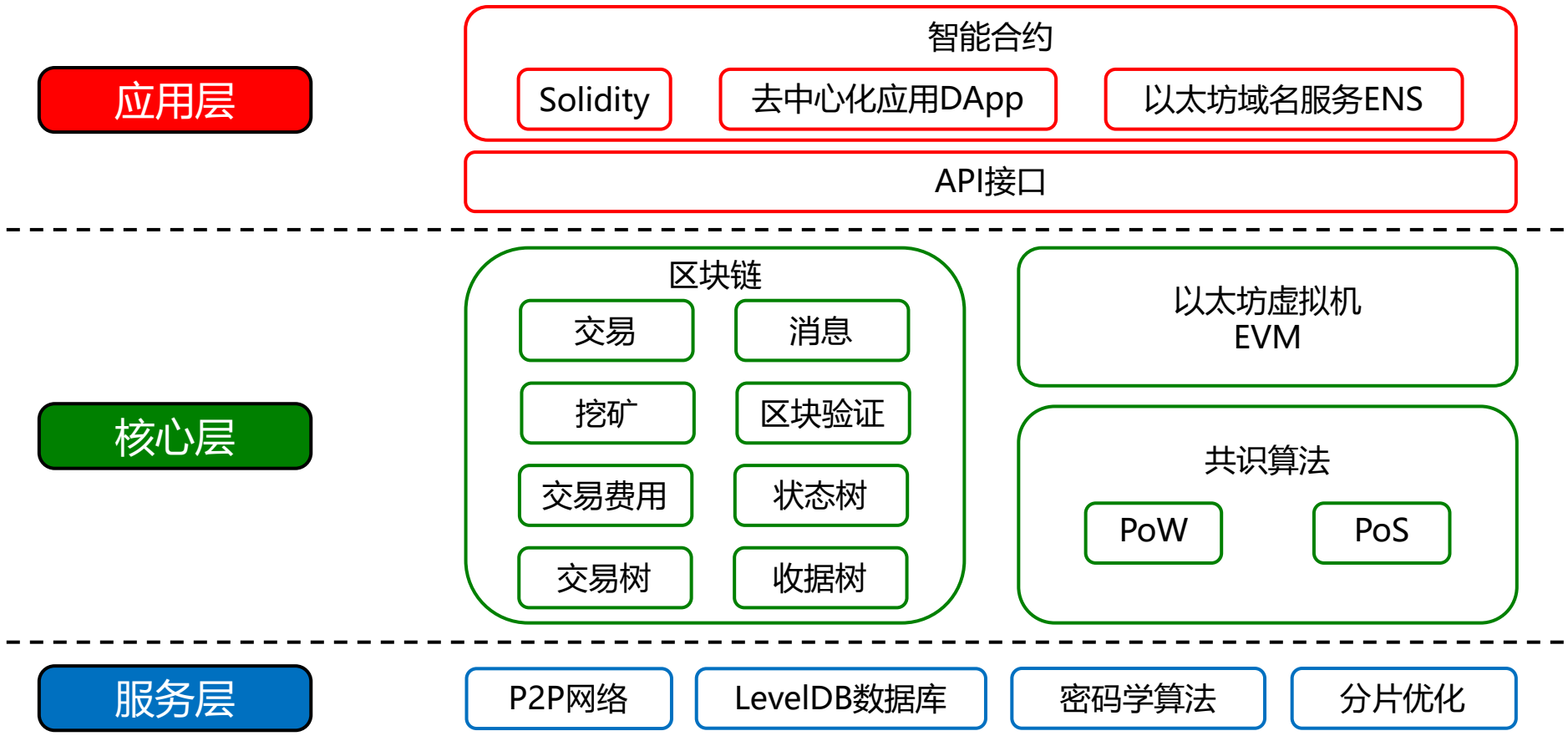
03 状态树、交易树与收据树

04 以太坊虚拟机

05 应用层

01 以太坊架构的概述

- 以太坊的主要架构可以分为三层：应用层、核心层和服务层。

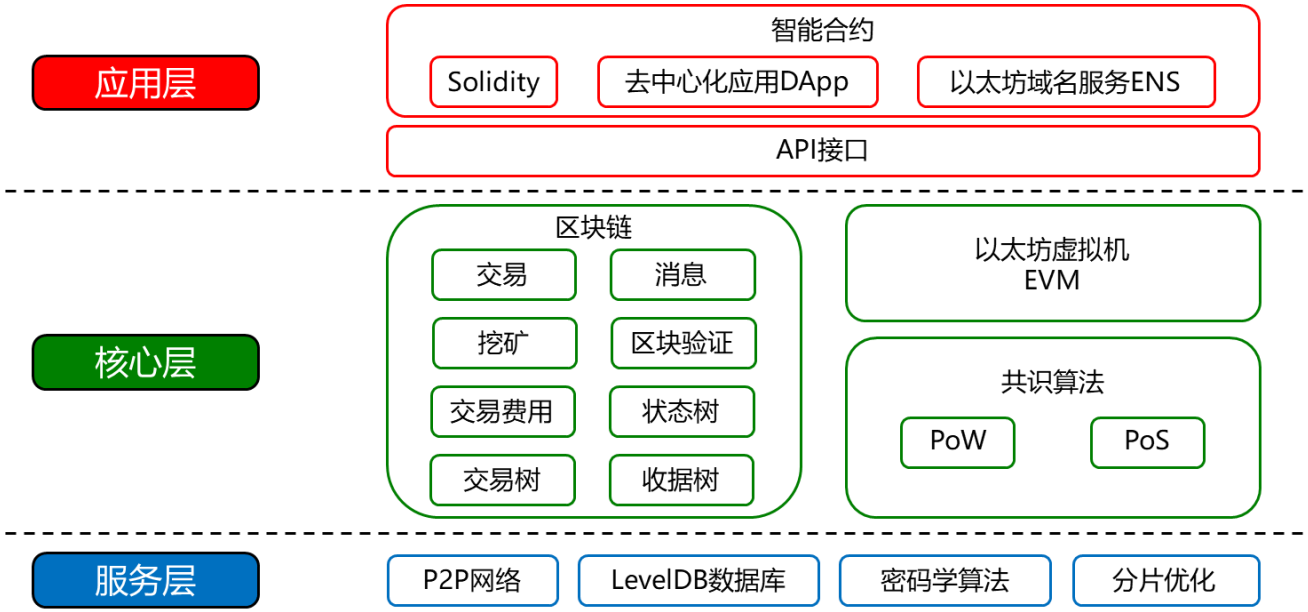


01 以太坊架构的概述

在应用层上，DApp通过Web3.js与智能合约进行信息交换。它是以太坊的最上层，即最接近用户的层。

核心层是以区块链技术为主体、以以太坊共识算法和以太坊虚拟机作为运行智能合约的载体的层。它是以太坊的第二层。

服务层包含P2P网络服务、LevelDB数据库、密码学算法以及分片优化等基础服务。它是以太坊的第三层。



02 服务层

- 服务层包含P2P网络服务、LevelDB数据库、密码学算法以及分片优化等基础服务，这些底层服务共同促使区块链系统平稳地运行。

服务层

P2P网络 P2P网络中每一个节点彼此对等，各个节点共同提供服务，不存在任何特殊节点，网络中的节点能够生成或审核新数据。

LevelDB数据库 以太坊中的区块、交易等数据最终都是被存储在LevelDB数据库中。

密码学算法 密码学算法用于保证数据的隐私性和区块链的安全性。

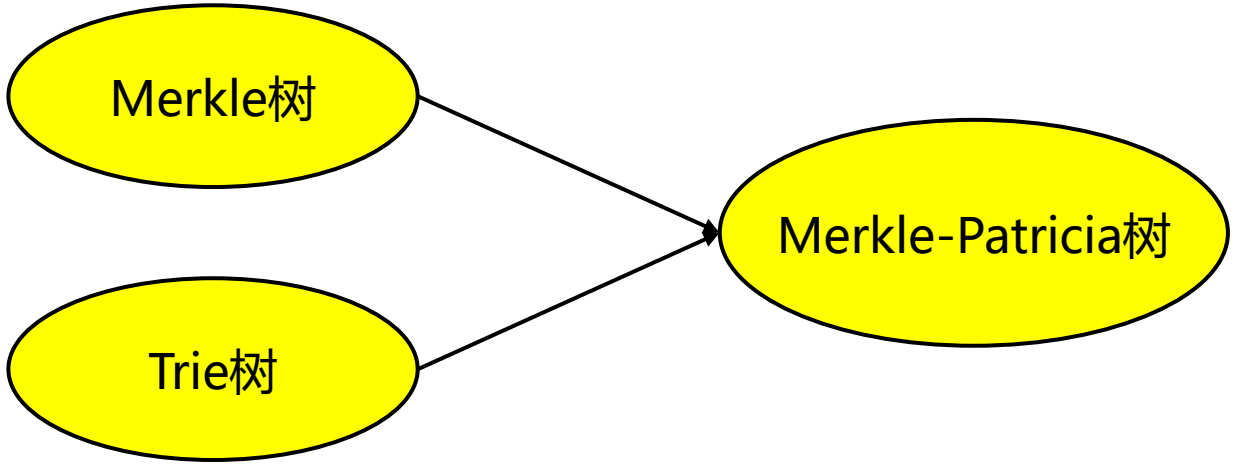
分片优化 分片优化技术使得并行验证交易成为可能，它大大加快了区块的生成速度。

03 状态树、交易树与收据树

- 在核心层中，以太坊针对三种对象设计了三种Merkle-Patricia树，它们分别是**状态树**、**交易树**与**收据树**。以太坊中采用Merkle-Patricia树来管理用户的账户状态、交易信息等重要数据。

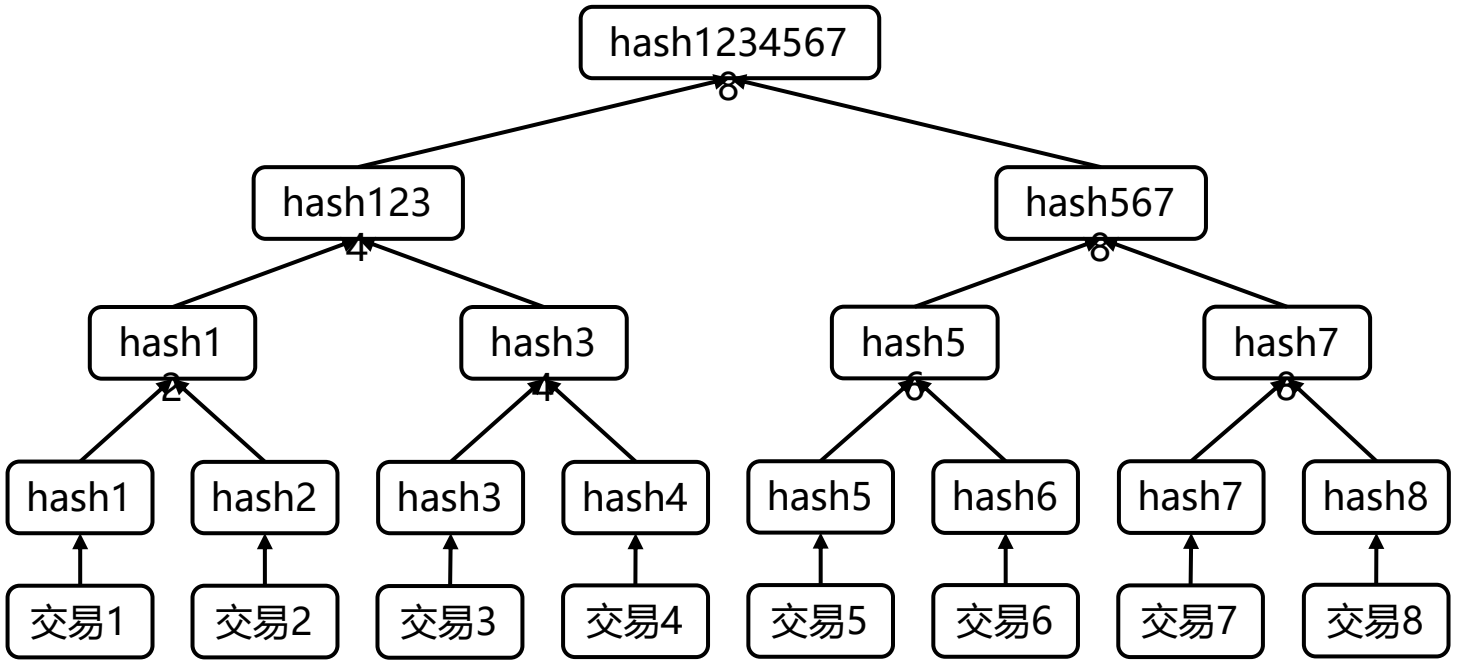
Merkle-Patricia树

Merkle-Patricia树是一种经过改良的树形数据结构，它融合了Merkle树和Trie树两种树形结构优点。



Merkle树

假设有8笔交易，则它们生成的Merkle树如下：

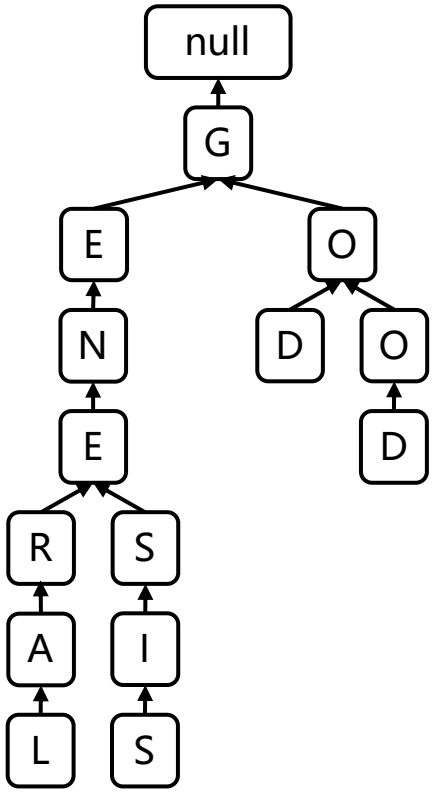


Merkle树有以下特征：

- 给定一个数据集，该数据集对应的Merkle树有唯一合法的根哈希值；
- 在Merkle树中更新、添加或删除叶子节点的效率较高，同时可以快速生成新的根哈希值；
- 如果用户可以提供一个特定叶子节点的分支，那么通过密码学方法证明叶子节点中包含的数据在该Merkle树中。

Trie树

假设现在有General、Genesis、Go、God、Good这几个单词，则它们生成的Trie树如下：



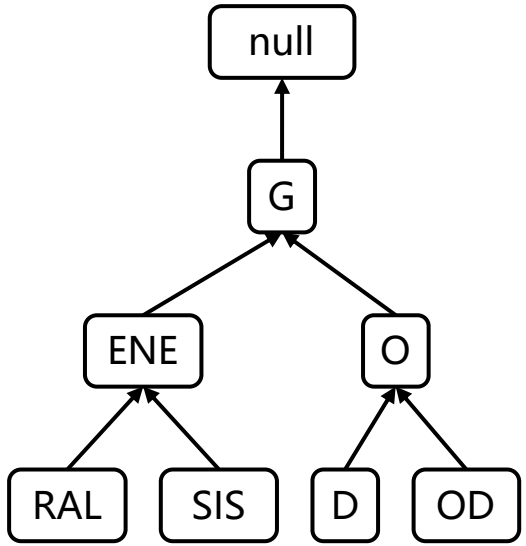
Trie树有以下特征：

- 如果数据有共同前缀，那么从中查询数据时十分高效；
- 如果数据没有共同前缀，那么从中查询数据时需要遍历整棵树，因此效率较低；
- 如果某数据没有与其他数据相同的前缀，那么存储该数据会造成空间浪费。

北京大学 PEKING UNIVERSITY

Patricia树

如果把上述的Trie树进行优化，即减少树的高度，就可以生成对应的Patricia树，如下图所示：



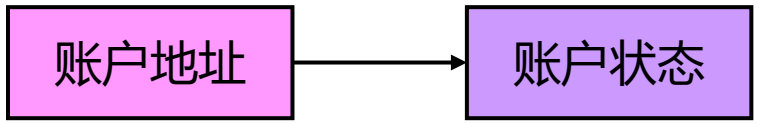
相比于Trie树，Patricia树有以下特征：

- 如果数据有共同前缀，那么从中查询数据时十分高效；
- 如果数据没有共同前缀，那么在Patricia树中大大减少了树的高度，因此Patricia树提高了这种情况的查找效率；
- 如果数据集越稀疏，那么这类数据集越适合使用Patricia树。
- 将Patricia树的叶子节点替换为哈希指针，即得到**Merkle-Patricia树。**

03 状态树、交易树与收据树

状态树

以太坊是基于账户的分布式账本，所以需要时刻记录账户的状态。状态树是记录账户状态的树形结构，因此需要将账户地址映射到账户状态，状态树中的数据形式是以上述映射为基础形成的键值对：



- 状态树有三种节点，包括**扩展节点**、**分支节点**和**叶子节点**。

扩展节点

扩展节点用浅绿色表示，它是用来保存路径的压缩数据的节点。

分支节点

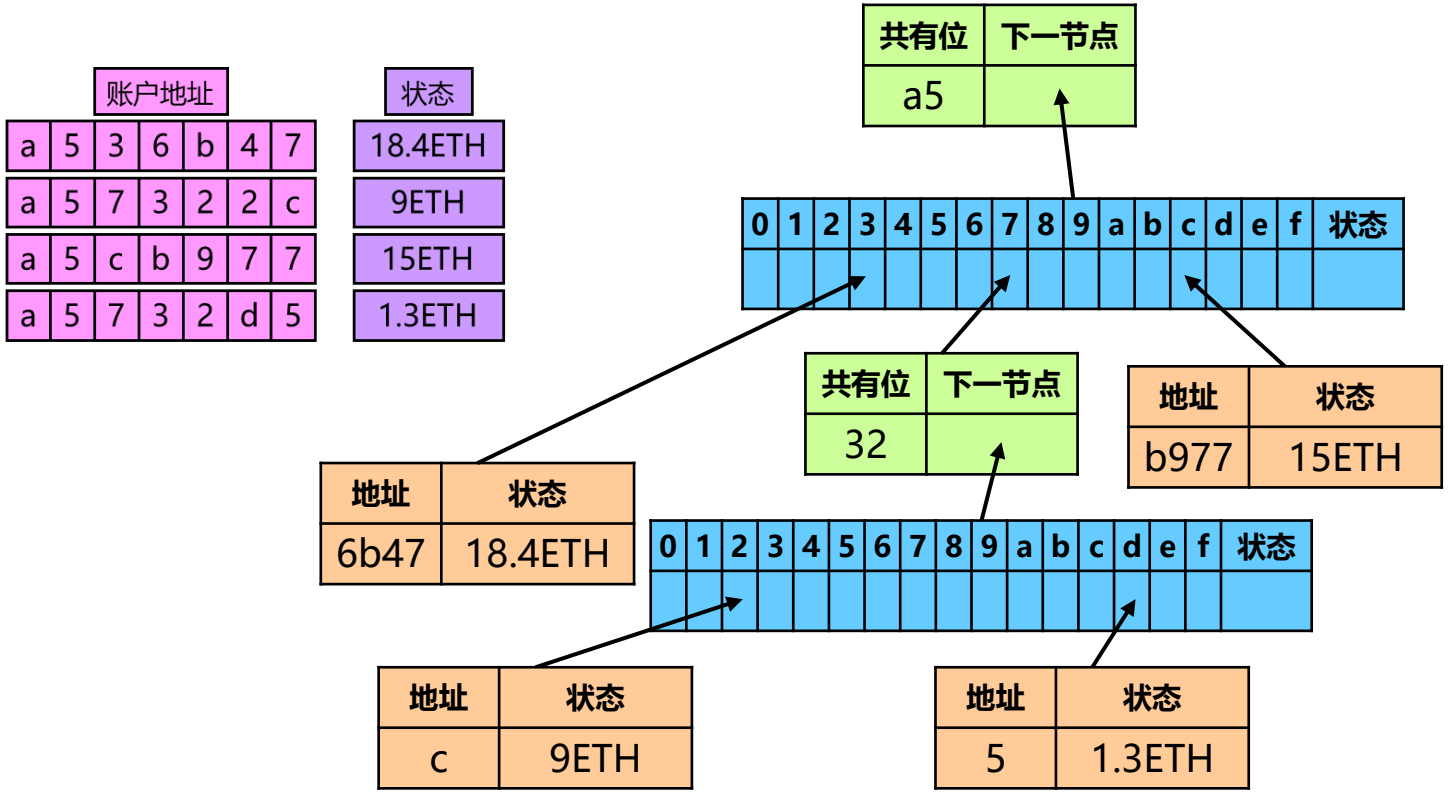
分支节点用浅蓝色表示，它共有17位，前16位表示十六进制数，最后1位表示终止与此节点的状态。

叶子节点

叶子节点用浅橘色表示，它是用来保存账户的最终状态的节点。

状态树

假设现在有下列四个账户地址，每个账户中存在对应的状态，那么这四个账户形成的状态树如下图所示：



状态树有以下特征：

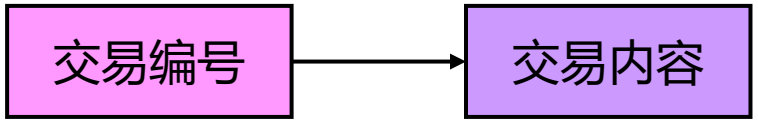
- 如果数据有共同前缀，那么从中查询数据时十分高效；
- 如果数据没有共同前缀，那么在Patricia树中大大减少了树的高度，因此Patricia树提高了这种情况的查找效率；
- 如果数据集越稀疏，那么这类数据集越适合使用Patricia树。
- 将Patricia树的叶子节点替换为哈希指针，即得到Merkle-Patricia树。

03 状态树、交易树与收据树

- 与**状态树**一样，**交易树**和**收据树**也是采用了Merkle-Patricia树的数据结构。

交易树

与比特币中的Merkle树作用类似，在以太坊中，区块内的交易列表形成交易树，每个区块都有一棵独立的交易树。区块中交易的顺序主要由矿工决定，在这个块被挖出前这些数据都是未知的。矿工一般会根据交易的GasPrice和nonce对交易进行排序。在交易树中，需要将交易编号映射到交易内容，交易数中的数据形式是以上述映射为基础形成的键值对：

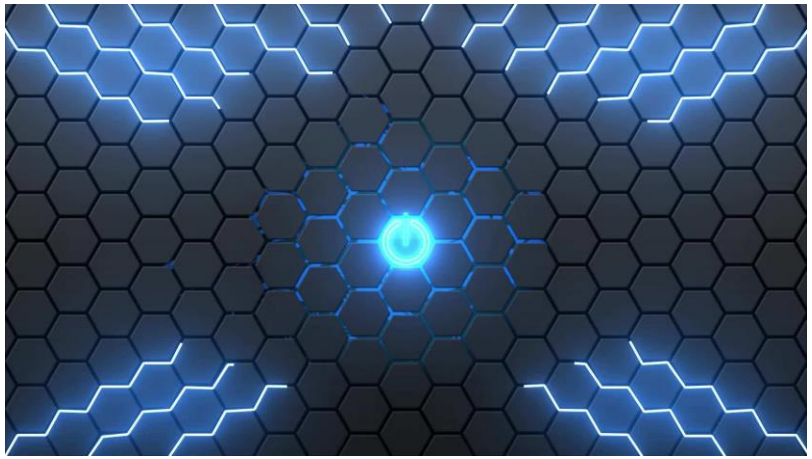


收据树

每个交易执行完后，会形成一个收据，该收据中包含一个布隆过滤器，它用来记录交易的相关信息。收据树中的每个节点与交易树中的节点是一一对应的。由于以太坊的智能合约执行过程比较复杂，增加收据树有利于快速查询交易的执行结果，因此以太坊引入了收据树的数据结构。

04 以太坊虚拟机

虚拟机通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的计算机系统。在实体计算机中能够完成的工作在虚拟机中都能实现。每个虚拟机都有独立的CMOS、硬盘和操作系统，可以像使用实体机一样对虚拟机进行操作。



以太坊虚拟机（EVM）是智能合约的运行环境，作为区块验证协议的一部分，参与网络的每个节点都会运行以太坊虚拟机，它可以被看做是一个大型的分布式计算机。以太坊虚拟机具有以下几个特性：

- 以太坊虚拟机具有封装性，它是一个完全独立的系统；
- 以太坊虚拟机具有隔离性，即在以太坊虚拟机具中运行的代码无法访问网络、文件系统和其他进程。
- 以太坊虚拟机具有图灵完备性。

北京大学 PEKING UNIVERSITY

图灵机

图灵机是“计算机科学之父”图灵在1936年提出的数学模型。他证明了如果可以实现图灵机，那么它可以解决任何可计算问题。图灵机的结构包括以下几个部分：

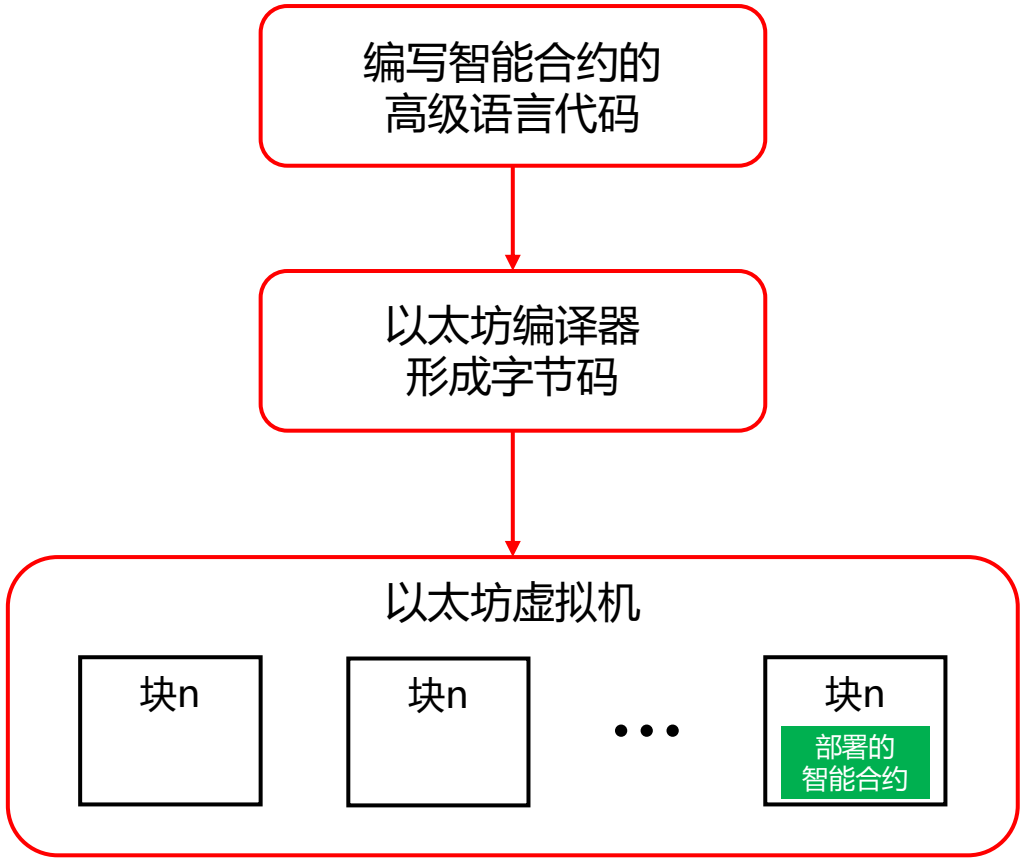
- **一条包含若干个格子的纸带**：每个格子可以包含至多一个字符，字符的集合表示纸带上可能出现的所有字符；
- **读写头**：它可以以操作格子上的字符，或者移动格子；
- **状态寄存器**：它追踪着每一步运算过程中，整个机器所处的状态；
- **有限的指令集**：它记录着读写头在特定情况下应该执行的行为。

图灵完备性

图灵完备性是针对一套数据操作规则而言的概念，在这里“数据操作规则”所指的对象是编程语言、指令集或虚拟机等。当“数据操作规则”可以实现图灵机模型里的全部功能时，就称它具有图灵完备性。

04 以太坊虚拟机

- 在编写智能合约时，智能合约与以太坊虚拟机的主要关系如下：



智能合约的编译流程如下：

- 智能合约的开发人员使用Solidity语言、Go语言等高级语言开发智能合约；
- 源代码在编译器中被编译成以太坊虚拟机支持的字节码，将其作为可执行程序；
- 开发人员将可执行程序部署到网络中，通过交易发布一个新智能合约，该合约账户会被打包到区块中；
- 外部账户或其他合约账户可以通过地址与该合约账户产生交易。

04 以太坊虚拟机

- 以太坊虚拟机与各组件有很密切的联系。

以太坊虚拟机与智能合约

- 智能合约通常是使用高级语言编写的，然后通过以太坊虚拟机编译器编译为字节码，最终通过客户端部署到区块链网络中。
- 智能合约以字节码的格式存在于区块链上。

以太坊虚拟机与账户

- 我们已经知道，以太坊中有外部账户和合约账户两类账户，它们共用以太坊虚拟机中同一个地址空间。
- 无论账户中是否存储代码或者余额，这两类账户对以太坊虚拟机来说处理方式是等价的。
- 每个账户在以太坊虚拟机中都以键值对的形式存储，其中键的长度和值的长度都是256位。

以太坊虚拟机与交易

- 交易可以看作是从一个账户发送到另一个账户的消息，它通常包含二进制数据和以太币信息。
- 如果目标账户含有代码，即目标账户是合约账户，那么此代码会在以太坊虚拟机中执行。这个过程就是调用智能合约的过程。
- 如果目标账户的账户地址为0，表示此交易将创建一个智能合约，该交易的二进制数据会被转换为以太坊虚拟机字节码并执行，执行的结果即作为智能合约上的代码，以太坊会永久存储这些代码。

05 应用层

- 应用层主要包括API接口、智能合约、去中心化应用DApp以及以太坊域名服务。

以太坊域名服务

- 以太坊域名服务（ENS）是一个区块链协议，它的目的是将加密地址缩短为人类可读的形式。
- 例如：现在有一串长地址“GhYESJnSKF47ndb3978OH3YNSSWED21”，这样的加密地址人们很难记住，这样的加密地址很难记住，以太坊域名服务可以将这样一串地址映射到一个短地址，例如Alice.eth。

智能合约

- 智能合约是以太坊的特性之一，可以说，以太坊的建立是为了智能合约而服务的。
- 智能合约是一种在区块链上运行的计算机程序，这段计算机程序是预先设计好的一套数字化规则，它包含真实世界经多方协商达成一致的业务逻辑。

去中心化应用

通常来说，不同的DApp会采用不同的底层区块链开发平台和共识机制。DApp是运行在分布式网络上的应用程序，参与者的个人信息能够被安全地保存在链上，这能够很好地保护用户的隐私。

第 4 节

以太坊交易

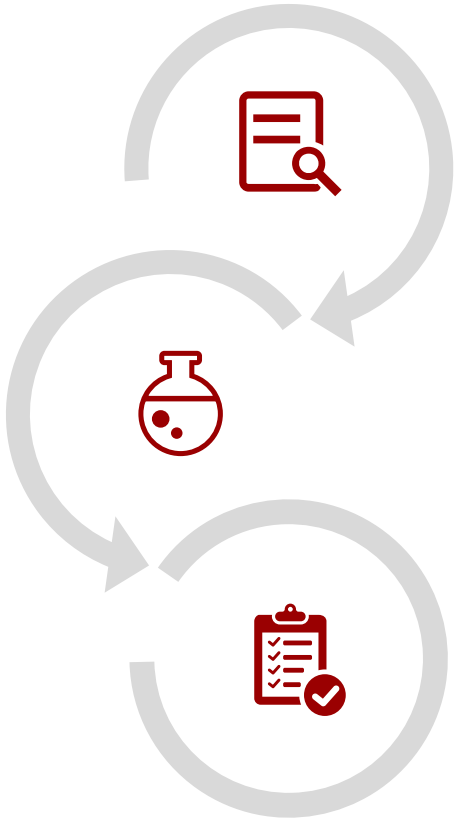
01 以太坊交易的类型

02 以太坊交易的结构

03 以太坊交易的过程

01 以太坊交易的类型

- 所有在以太坊中的交易大致可以分为三类：**转账交易、创建合约的交易、执行合约的交易。**



转账交易

转账交易是最简单、最常见的交易，即一个账户向另一账户发送以太币产生的交易。

创建合约的交易

创建合约的交易指的是将合约部署在区块链上的交易，这是外部账户通过发送交易来实现的。

执行合约的交易

执行合约的交易是为了执行已经部署在区块链上的智能合约。在这种交易中，交易的发送方是要调用智能合约的账户地址，交易的接收方是智能合约的地址。

02 以太坊交易的结构

北京大学 PEKING UNIVERSITY

- 在以太坊中发生的交易对应的数据结构包括以下字段：

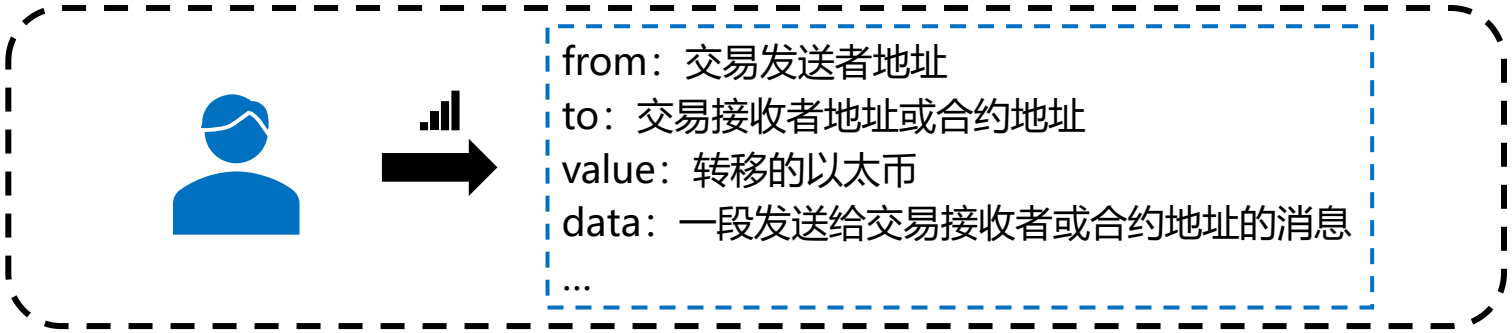
字段名称	含义
nonce	数量
gasPrice	交易发送者希望在这笔交易中支付每单位gas的价格
gasLimit	交易发送者希望在这笔交易中花费gas数量的上限
to	若为转账交易，表示交易接收者的地址； 若为创建合约的交易，此字段为空
value	若为转账交易，表示转移给交易接收者比特币的数量； 若为创建合约的交易，表示为新合约的初始捐款
v	由交易发送者的私钥对交易签名生成的1字节数据
r	由交易发送者的私钥对交易签名生成的32字节数据
s	由交易发送者的私钥对交易签名生成的32字节数据
data	如果该字段存在，表示该交易是创建合约的交易或调用合约的交易

03 以太坊交易的过程

- 与普通的银行转账不同，在以太坊中，处理交易并不是瞬间完成的，而是存在一个过程。从账户发起交易请求开始、到包含该交易的区块达成共识为止，满足这个过程才算完成一笔交易。
- 本小节将分两种情况介绍以太坊交易的过程，**转账交易与执行合约的交易**有相似的交易过程，**创建合约的交易**的过程与前者相比有些不同。

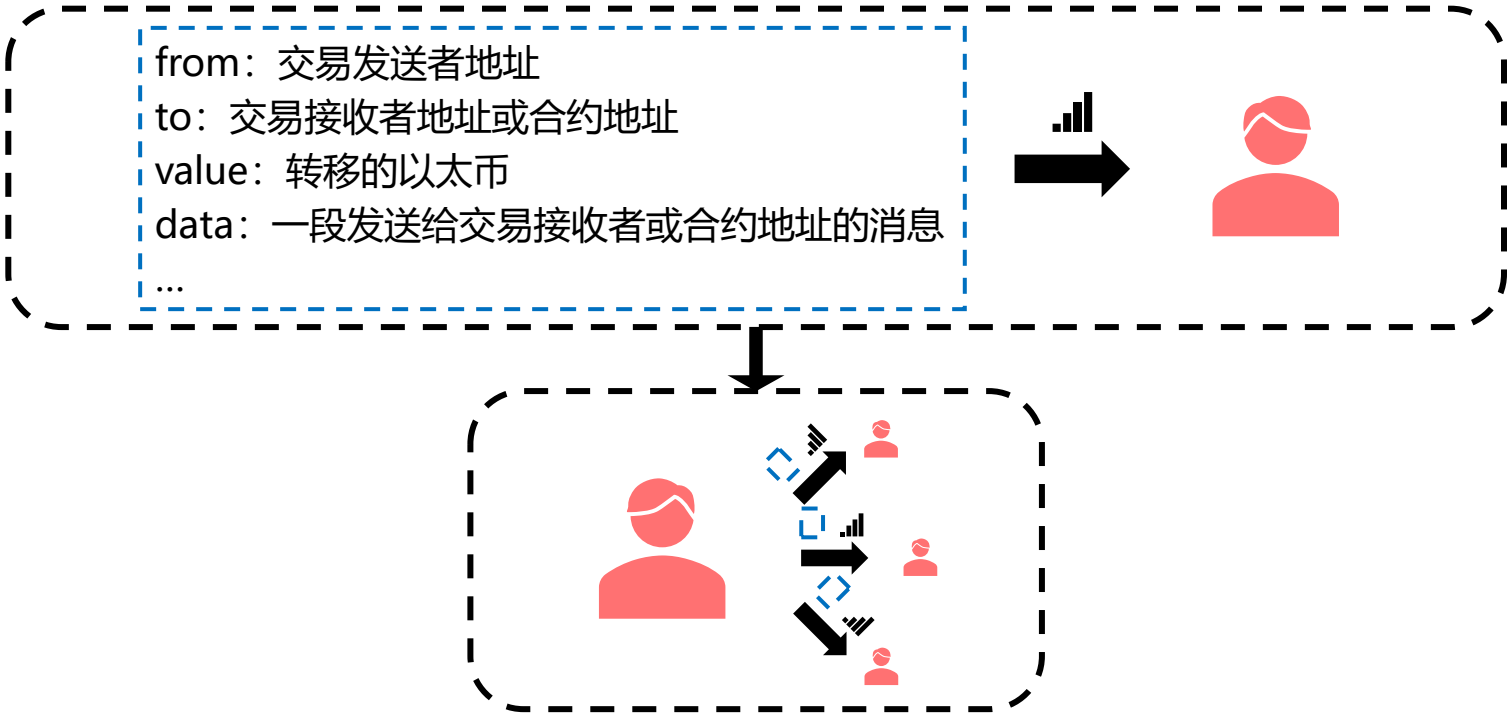
转账交易与执行合约的交易的交易过程

1. 发送交易请求。交易发送者（蓝色人像）按照既定的交易格式在以太坊中发起一个交易请求，随后该请求被传向交易发送者的对等节点。



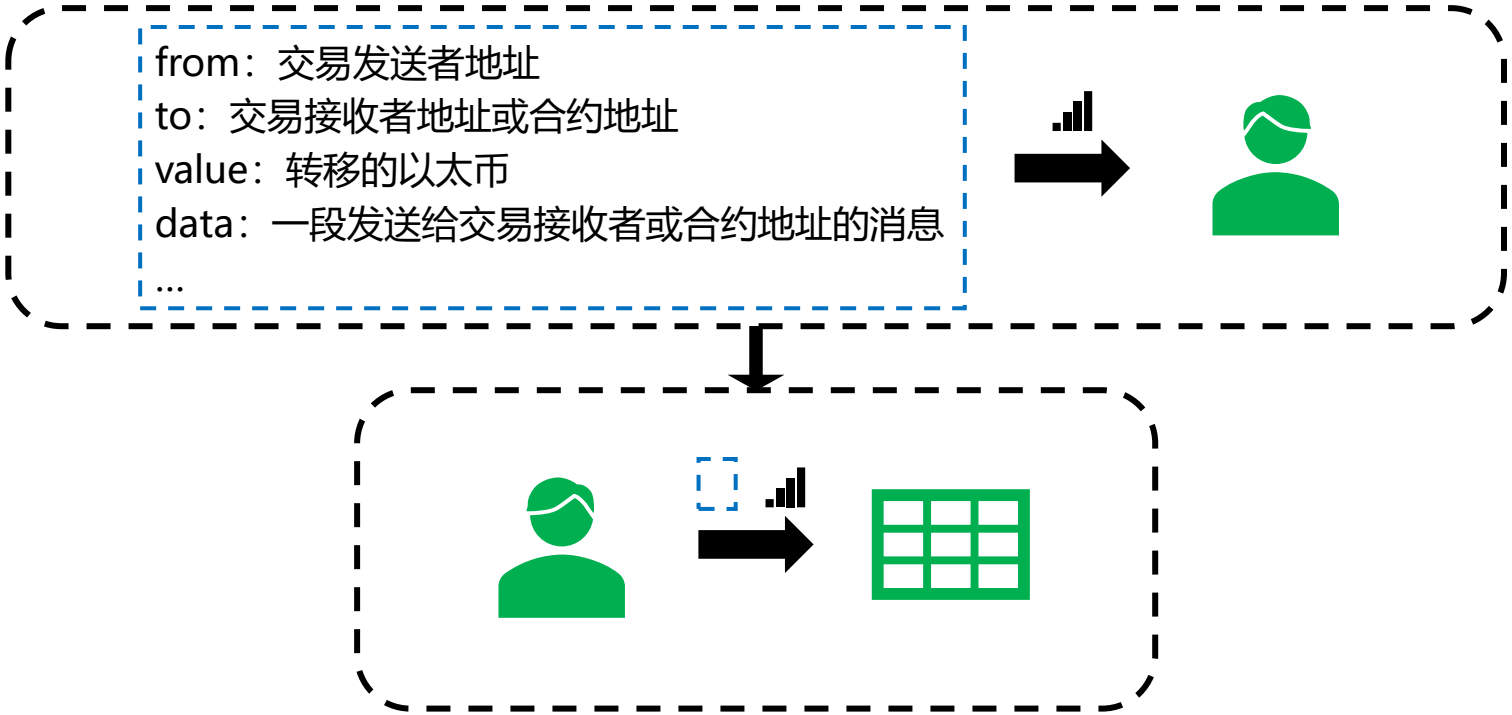
03 以太坊交易的过程

2. 验证交易请求并广播。以太坊网络中的节点（红色人像）同步了此交易，它会检查交易是否有效、格式是否正确、确定发送方的地址。如果符合要求，则计算可能的最大交易费用，并在本地的区块链上减去相应的费用。对符合要求的交易请求，以太坊网络中的节点会将其放在交易存储池中，并且转发给其他节点。其他收到交易请求的节点重复该节点的处理过程。



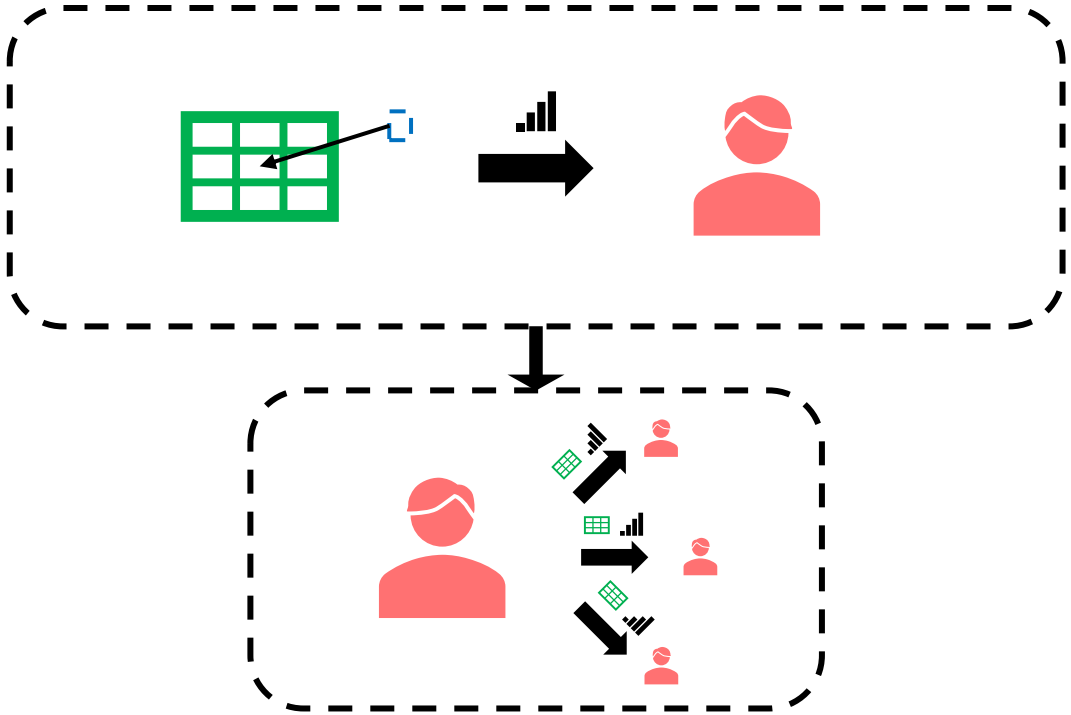
03 以太坊交易的过程

3. 矿工打包交易或执行合约。对于转账交易，矿工（绿色人像）将该交易和其他交易一起打包到区块中；对于执行合约的交易，矿工将该交易和其他交易一起打包到区块中，并在本地的以太坊虚拟机中执行被调用的合约代码，直到代码执行完毕或gas耗尽。如果代码还没有执行完毕而gas已经耗尽，那么所有状态回滚到代码执行之前，但是已经消耗的gas不可收回，交易费用由矿工获得。如果代码执行完毕后gas还有剩余，那么矿工也只会获得消耗的gas。



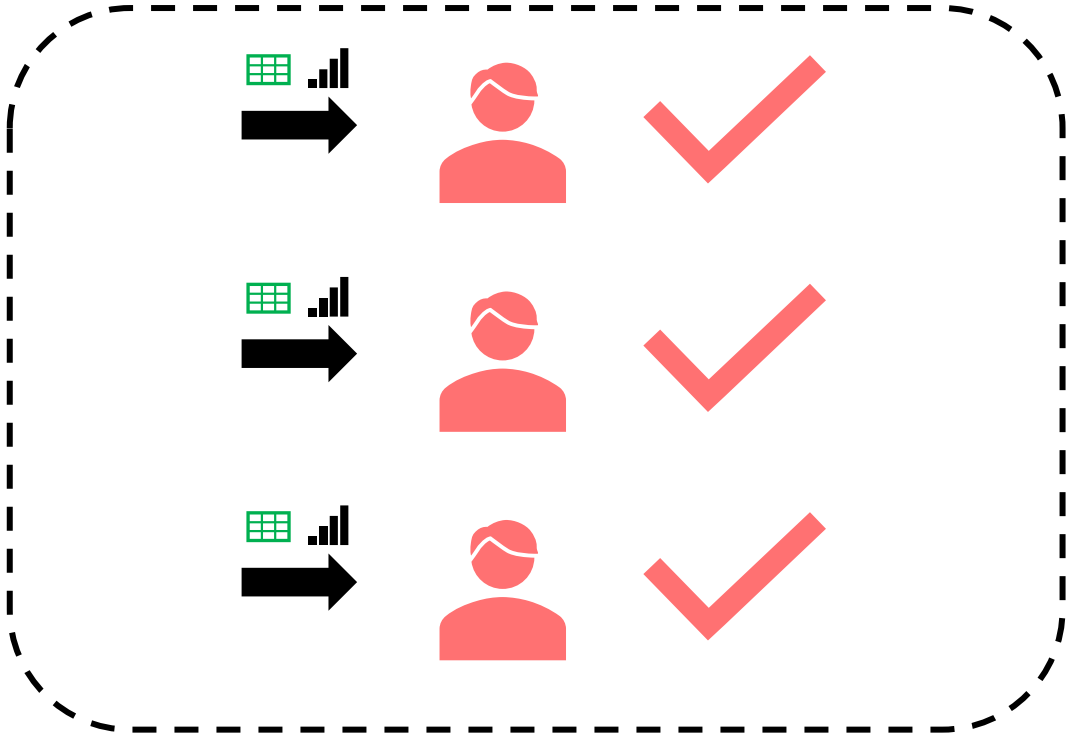
03 以太坊交易的过程

4. 广播区块。以太坊网络中的节点把包含交易发送者的交易请求的区块发送至以太坊网络中的其他节点，并在网络中传播。



03 以太坊交易的过程

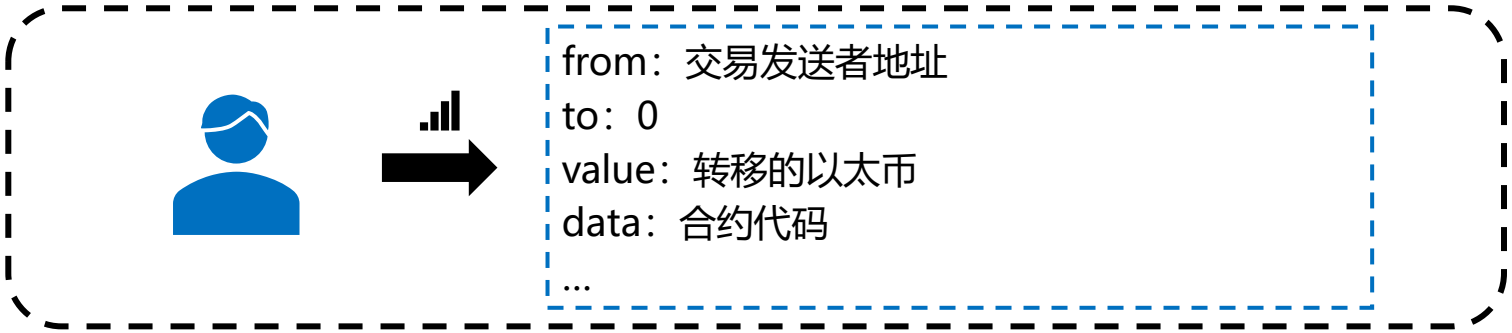
5. 验证区块并同步。其他节点收到该区块后，验证该区块的合法性，如果区块通过验证，节点将内存池中原来交易发送者的交易请求删除，同时同步该区块，将其添加到本地的区块链中。对于区块中的执行合约的交易，其他节点会在本地的以太坊虚拟机中执行该智能合约，并验证运行的结果。



03 以太坊交易的过程

创建合约的交易的交易过程

1. 发送创建合约的交易的请求。交易发送者按照既定的交易格式在以太坊中发起一个交易请求，随后该请求被传向交易发送者的对等节点。



03 以太坊交易的过程

2. 验证交易请求并广播。以太坊网络中的节点（红色人像）同步了此交易，它会检查交易是否有效、格式是否正确、确定发送方的地址。如果符合要求，则计算可能的最大交易费用，并在本地的区块链上减去相应的费用。对符合要求的交易请求，以太坊网络中的节点会将其放在交易存储池中，并且转发给其他节点。其他收到交易请求的节点重复该节点的处理过程。

3. 矿工将该交易和其他交易一起打包到区块中，然后根据其提供的交易费用和合约代码，创建合约账户并部署合约。合约账户的地址是由交易发送者的地址和nonce值作为输入通过加密算法生成的，待交易确认后将合约账户的地址返回给交易发送者。

03 以太坊交易的过程

4. 广播区块。以太坊网络中的节点把包含交易发送者的交易请求的区块发送至以太坊网络中的其他节点，并在网络中传播。

5. 验证区块，并部署智能合约到本地。共识节点接收到该区块，验证该区块的合法性，如果区块通过验证，节点从内存池将原来交易发送者创建合约的交易请求删除掉，并将智能合约部署在各自的本地区块链中。

一般来说，当包含交易的区块链被同步到区块链后，出于安全性的要求，还需要再挖出一些区块，这笔交易才能算是真正地被确认。

第5节

DApp开发

01 DApp概述

02 DApp架构

03 开发DApp的过程

04 truffle框架

05 Ganache区块链网络

01 DApp概述

互联网是一个去中心化的网络。相较于传统客户端/服务器模型，互联网的巨大优势在于其提供了开放、透明、公平的竞争环境。更多的竞争意味着更多的创新，这最终体现在为消费者提供更好的用户体验。

与传统的应用程序不同，DApp的数据和逻辑存储在公有链上。在智能合约中，数据和操作可以精细化到只允许特定的账户访问，从而实现了个人的数据所有权。由于核心数据和逻辑位于公链上，因此任何用户都可以创建和部署前端应用程序，这就是DApp名字的由来。

01 DApp概述

- DApp有三个特性：弹性、透明性、抗审查性。

弹性

与在中央服务器上部署应用程序不同，DApp不会有停机时间，只要以太坊在运行，那么DApp就会持续执行。

透明性

DApp的透明性意味着它允许任何节点发布代码，任何与区块链的交互都将被永久存储，区块链网络上的任何节点都可以获得对它的访问权限。

抗审查性

如果用户可以访问以太坊节点，那么将始终能够与DApp交互。一旦节点在网络上部署代码，任何节点都没有更改代码的权限。

01 DApp概述

北京大学 PEKING UNIVERSITY

- DApp与中心化应用对比，具有以下几个特点：

	中心化应用	去中心化应用
代码开源	不开源	完全开源
数据存放	中心化存储	在智能合约中存储
公平性	不透明化，存在暗箱操作的可能	公平公正
运行效率	取决于服务器的配置	取决于公链节点
手续费	不需要手续费	需要手续费

02 DApp架构

- DApp的架构可以简单分成三种类型：轻钱包模式、重钱包模式和兼容模式。

轻钱包模式

轻钱包模式的DApp需要有一个开放的HTTP/RPC协议的节点与钱包通信，这个节点可以是任意区块链上的节点。轻钱包模式的DApp通常会作为一个浏览器插件存在，插件在运行时会自动注入Web3框架，DApp可以通过Web3与区块链节点通信。

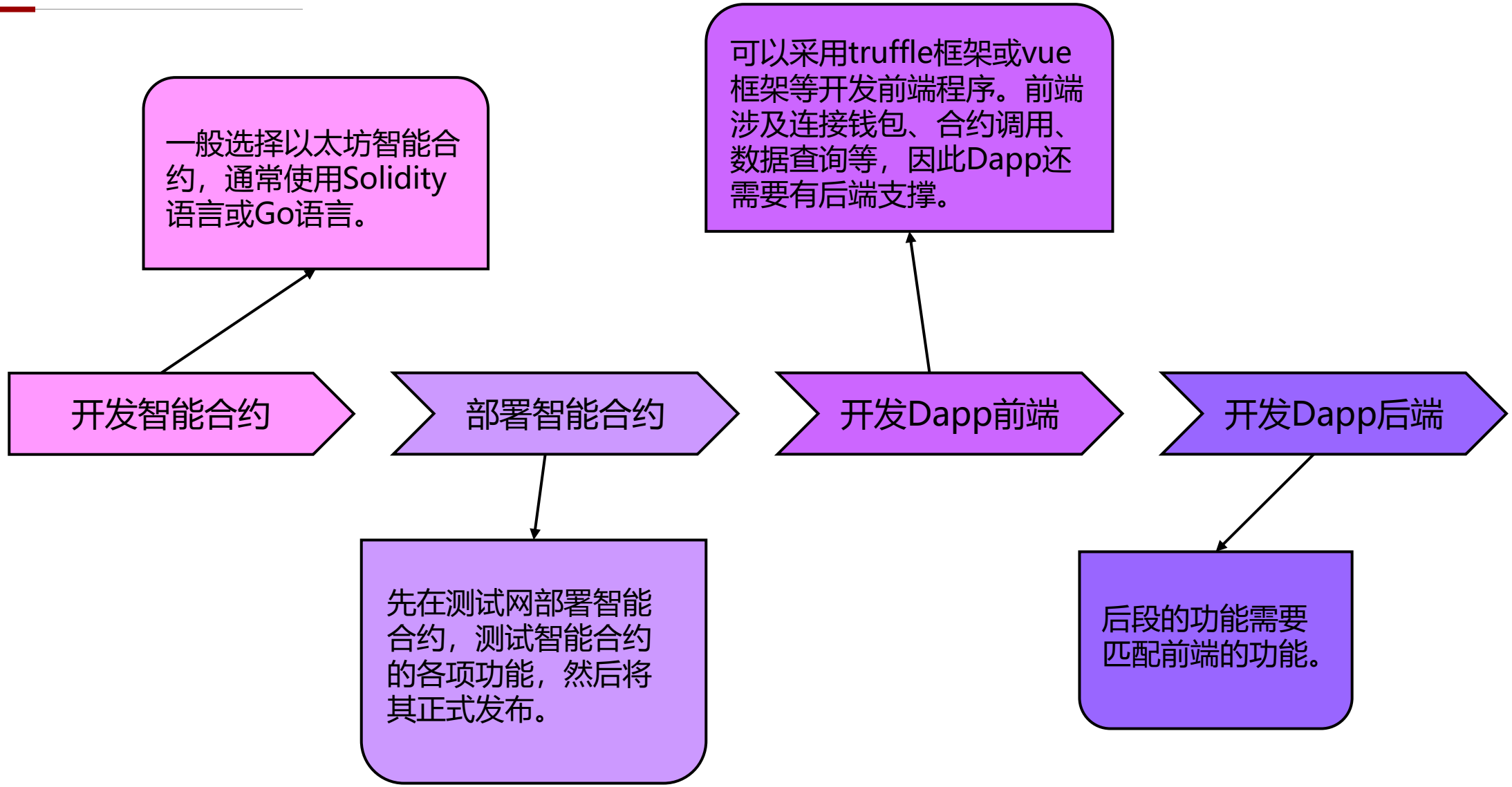
重钱包模式

重钱包模式的DApp会自动同步并持有一个区块链节点，并提供一个浏览器环境。

兼容模式

兼容模式的DApp可以在轻钱包模式和重钱包模式下同时使用，与钱包通信的节点可以在本地持有，也可以自己搭建服务持有并公布节点。

03 开发DApp的过程



04 truffle框架

- truffle框架是基于Solidity语言的一套开发框架。

truffle开发框架提供了很多功能，它简化了用户的开发、编译、部署与调试过程，总体来说，它有以下特性：

- 内置了智能合约编译、链接、部署和二进制文件的管理的功能；
- 方便快速开发合约，同时支持自动化测试合约的功能；
- 方便网络管理功能；
- 内置控制台功能，在项目构建后，可以直接在命令行调用输出结果；
- 支持执行外部脚本。

05 Ganache区块链网络

- Ganache是一个可以在本地部署的区块链网络。

- Ganache区块链网络是一个基于以太坊的个人开发环境，用户可以在上面部署合约、开发程序和进行测试。它提供了很多种版本，包括桌面版本、命令行工具版本等。总的来说，它是一个本地化的以太坊网络。
- 使用Ganache区块链网络进行开发最大的特点是响应速度快。开发以太坊上的DApp一般在测试网上进行，虽然测试网的响应速度相对主网而言比较快，但是还是存在拥堵的情况，那么用户使用本地化的以太坊网络就没有这个限制了。这不仅为用户节省了大量开发时间，也使用户的开发节奏更为连贯。

本章小结

本章主要围绕以太坊展开。

- 第1节从以太坊的概念、发展历史、关键组件和应用举例等角度简要介绍了以太坊。
- 第2节简要介绍了以太坊账户的相关概念，包括以太坊的地址、以太坊的钱包、以太币等概念
- 第3节简要介绍了以太坊的架构账户，分别介绍了服务层、核心层、应用层中所应用的技术及原理。
- 第4节简要介绍了以太坊交易的相关概念，包括以太坊交易的类型、以太坊交易的结构与以太坊交易的过程。
- 第5节介绍了DApp开发相关知识，简要介绍了DApp架构和DApp的开发过程，最后介绍了两种开发DApp的工具。

北京大学
PEKING UNIVERSITY

感 谢 您 的 观 看