Node 区块链加速器

区块链与创新创业

http://www.node.ac

李晋

西安电子科技大学 通识课程 2021春季学期

一 上次课回顾

- 区块链1.0：比特币简史
- 比特币工作原理
- 工作量证明、挖矿
- 比特币的特性
- 如何获取和使用比特币
- 加密数字货币的经济学基础
- 区块链1.0时代的一些典型替代币

Node 区块链加速器

PART 3
区块链2.0：以太坊、DApp与智能合约

一 区块链1.0的应用尝试与2.0的开端

- Namecoin：诞生于2010年，去中心化的域名系统。利用区块链实现名称注册系统的最早的、较为成熟的系统
- Mastercoin即Omni协议：第一个ICO项目。一种Colored coins（染色币/彩色币），为人们在比特币区块链上创建自己的数字货币，利用比特币已有的区块链网络基础。人们可以通过为某一特别的比特币UTXO指定颜色，发行新的货币。（后来Bitfinex发行的USD Tether即基于Omni，BCH上也基于Omni协议尝试了Wormhole虫洞协议）
- BitShares：采用DPoS共识算法，最早的去中心化交易所。创始人也是Steem和EOS的创始人Dan Larimer（BM）
- Counterparty：合约币，基于比特币区块链，实现交易合约
- Rootstock：致力于在Bitcoin上实现DApp及智能合约

3.1 以太坊的诞生与设计目标

一 以太坊Ethereum的诞生

- 2014年1月，19岁小伙Vitalik Buterin发布以太坊白皮书“Ethereum: A Next Generation Smart Contract & Decentralized Application Platform”
- 设计目标：区块链怎样应用于货币以外的领域——把区块链变成计算机，上面运行DApp程序，并实现智能合约
- 2014.7发起众筹，筹得 31529 BTC（当时价值约$1200万美元）

Ethereum White Paper

A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM

By Vitalik Buterin

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 digital currency. Satoshi's blockchain was the first credible decentralized solution. And now, attention is rapidly starting to shift toward this second part of Bitcoin's technology, and how the blockchain concept can be used for more than just money.

Commonly cited applications include using on-blockchain digital assets to represent custom currencies and financial instruments ("colored coins"), the ownership of an underlying physical device ("smart property"), non-fungible assets such as domain names ("Namecoin") as well as more advanced applications such as decentralized exchange, financial derivatives, peer-to-peer gambling and on-blockchain identity and reputation systems. Another important area of inquiry is "smart contracts" - systems which automatically move digital assets according to arbitrary pre-specified rules. For example, one might have a treasury contract of the form "A can withdraw up to X currency units per day, B can withdraw up to Y per day, A and B together can withdraw anything, and A can shut off B's ability to withdraw". The logical extension of this is decentralized autonomous organizations (DAOs) - long-term smart contracts that contain the assets and encode the bylaws of an entire organization. What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.

Node 区块链加速器

3.2
以太坊原理与关键技术

一 以太坊基本原理

- 比特币定位为电子现金（货币），不需要过多功能。脚本语言限制很大，尤其不直接支持loop，对数字货币来说够用，但对于去中心化计算机，缺乏灵活性和足够的抽象层次
- 以太坊将区块中存储的数据不再只是币的转账数据，还可以存放程序代码及变量状态
- 虚拟机EVM：抽象，屏蔽底层细节，上层类似通用计算机的能力
- 支持使用Solidity等高级语言编写DApp软件，称为“图灵完备”语言
- Ether（以太币）作为原生coin。运行DApp程序需要花费gas，避免浪费计算资源和攻击
- 由于DApp是在去中心化的可信环境中执行，因此具备了实现“智能合约”的能力
- 以太坊采用PoW，但修改了挖矿算法，抗ASIC，适合用显卡挖矿，目前尚无专用ASIC矿机
- 与Bitcoin的UTXO架构不同，以太坊使用了account

Node 区块链加速器

3.3
智能合约

智能合约 Smart Contract

- 能够以信息化的方式签订、执行合同，能够根据事先任意制订的规则来自动转移数字资产，无需第三方监督或公证，且交易不可逆转——触发某条件，程序自动执行资产转移

```
If Event_X_Happened():
    Send(爱丽丝, 1000$)
Else:
    Send(鲍伯, 1000$)
```

- 早在1994年由Nick Szabo提出，一直未能实现——缺乏可信执行环境
- 以太坊为智能合约提供了绝佳的底层可信执行环境：代码被部署在区块链的分布式账本上，参与的多方共同见证其按设计者的意图自动执行，所有用户可见、不可篡改
- Code is law 代码即法律

智能合约 Smart Contract

- 基于智能合约，以太坊提出了DAO（decentralized autonomous organization）、DAC（decentralized autonomous corporation）的实现可能
- 将可编程数字金融往前大大推进了一步

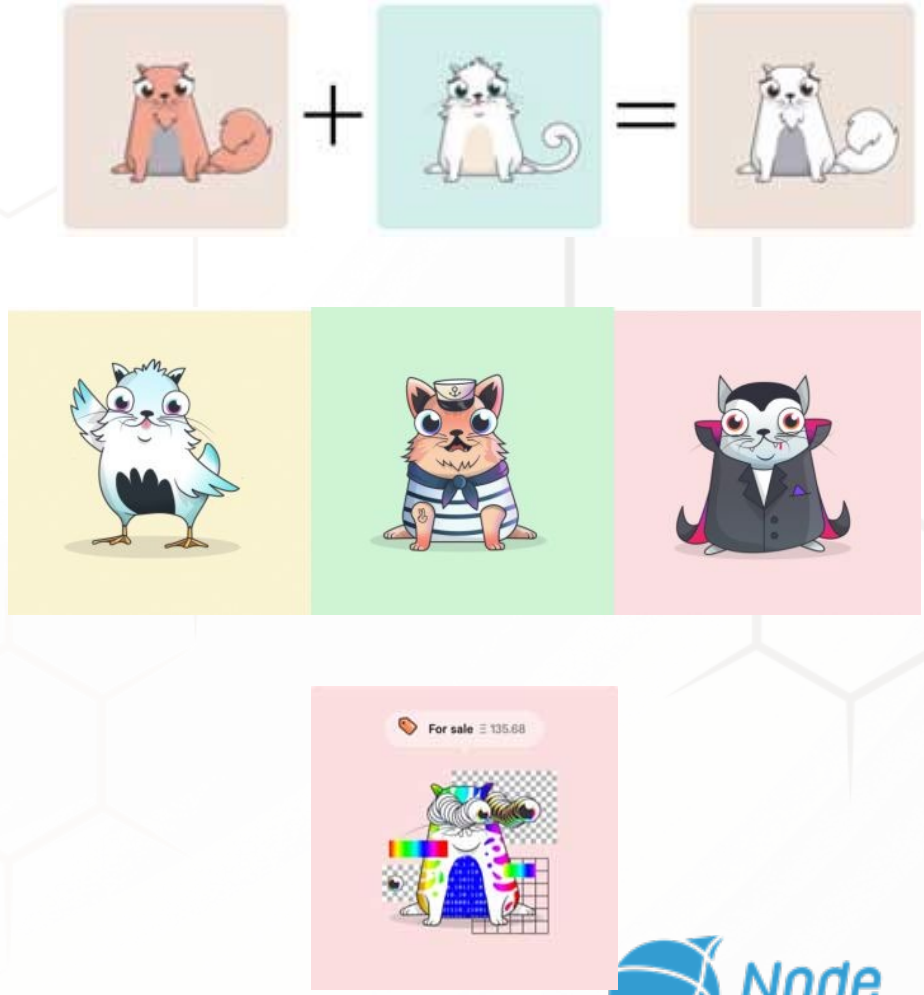
Node 区块链加速器

3.4
DApp举例：Crypto Kitties

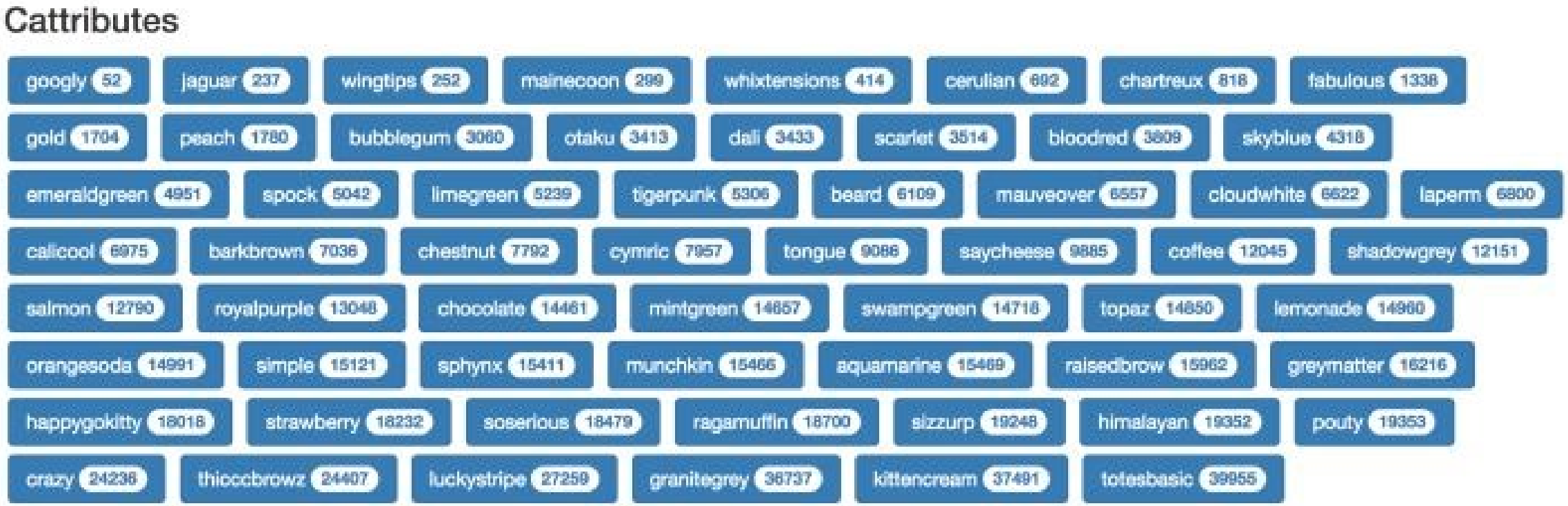
Crypto Kitties 加密猫

- https://www.cryptokitties.co/
- 加拿大游戏工作室 Axiom Zen 开发。2017年11月28日上线
- 有100只系统自己创建的“创世猫”，每15分钟就有一个新的0代猫诞生
- 用户需先买两只不同的猫，进行交配生小猫，小猫也可以再繁殖
- 猫可以用ETH自由买卖，采用荷兰式拍卖机制，定价区间内价格随时间流逝下降。开发者从每笔买卖中自动获取3.75%的费用
- 每只猫都有256位的基因组，代表不同特点，如某部分颜色、胡须、花纹、生育恢复时间。还有隐形基因，看不出来。越稀缺的基因越贵
- 用户赋予的创意、包装也会影响价格，比如起名，及对稀有属性的概念包装

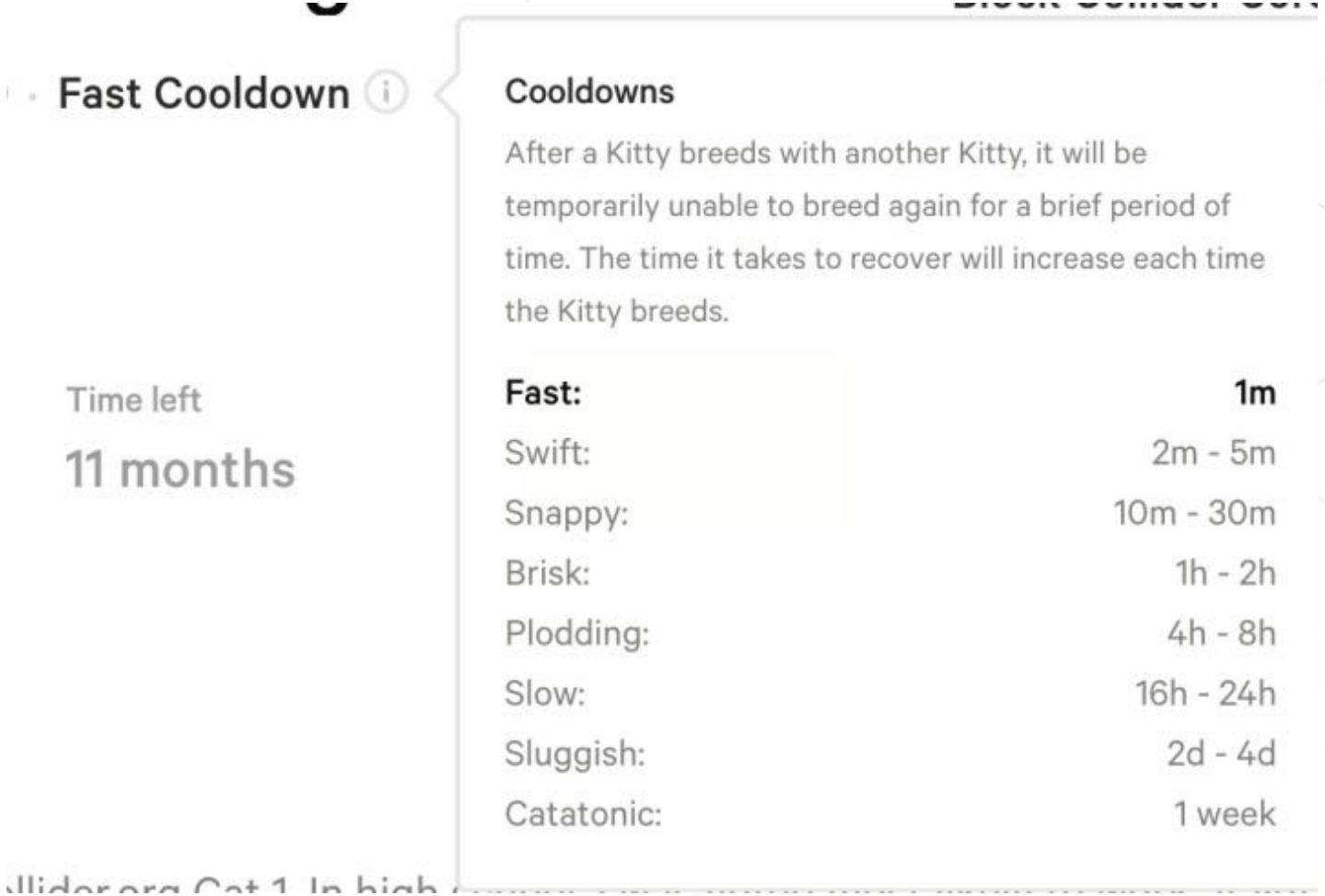
Crypto Kitties 加密猫



Crypto Kitties 加密猫



Crypto Kitties 加密猫



Crypto Kitties 加密猫

- 火爆的原因除了创意，更多源于投机性，击鼓传花
- 最贵的一只猫曾经交易价格折合人民币77万（现在几乎一文不值）
- 数字猫是一种“非同质化代币”（Non Fungible Token，NFT），其遵循了 ERC721 标准
- 区块链和非区块链结合，渲染展示部分是中心化的

Crypto Kitties 与传统养宠物游戏有何区别?

- 代码开源，部署到区块链上之后，所有人都能看到（并认同规则，达成共识），所有人都无法更改规则（包括开发者）
  - 你的猫（资产）别人永远拿不走，也不会因为“停服”而消失
  - 谁也没法通过后门捷径制造猫，公平公开
- 传统养猫部署在中心化服务器上，规则、数据记账权是开发商掌握，发行资产、代管资产都无法由大众监督

总结

- 现象级产品，超棒的创意和设计，引发了大家对DApp的无限期待和创新，尤其游戏领域，此后又出现了更加夸张的 Fomo3D 资金盘游戏
- 瞬时间引发以太坊网络瘫痪，交易确认极慢、手续费极高，暴露出以太坊网络目前吞吐量太低，无法支撑大规模应用
- 对普通用户来说易用性差（需要先有ETH，需要用MetaMask浏览器插件），限制了用户基数
- 开发者无法升级，所以如果投放运行前没有设计好规则，或代码有漏洞，将没有机会修改弥补
- Fomo3D被黑客攻击导致游戏中止，再次体现了智能合约代码安全性的问题
- 此应用很好的展示了DApp的特点
- 近几个月NFT引领了又一波狂热的击鼓传花游戏

Node 区块链加速器

3.5
以太坊发展历程

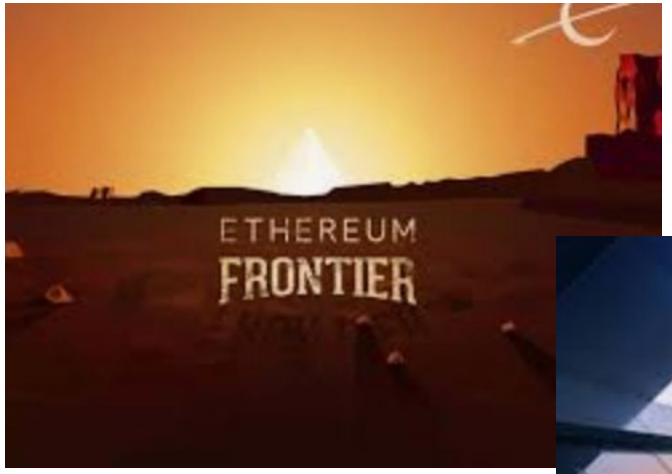
以太坊创始人Vitalik Buterin

- 江湖称其“V神”
- 1994年出生于俄罗斯
- 1998年，年仅4岁开始编写程序
- 2006年，编写C++代码
- 2011年，联合创办《Bitcoin Magazine》，担任首席撰稿人
- 2013年，大一即从滑铁卢大学休学
- 2014年1月，发布以太坊白皮书
- 2014年7月，众筹3.1万个比特币，并成立以太坊基金会
- 知识渊博，涉猎广泛，中文说的非常不错
- https://vitalik.ca/

以太坊发展历程

- 2015年，以太坊PoC概念验证测试网络，称为Olympic版本
- 2015年7月30日，以太坊 Frontier 版本上线， 宣布了以太坊系统的正式诞生
- 2016年3月14日（圆周率节），以太坊进入 Homestead 阶段
- 2016年6月，以太坊上的一个去中心化自治组织 The DAO 被攻击，导致市值5千万美金的以太币被盗，最终Vitalik提出回滚并产生了硬分叉，自此以太坊分为了ETH和ETC（Ethereum Classic），引起巨大争议，也反映了智能合约的缺点
- 2017年10月，以太坊进入 Metropolis 阶段的一阶段 Byzantine
- 2018年1月，以太坊市值创历史高点
- 升级进度缓慢，技术持续挑战，社区共识难以达成
- 2020年，终于启动Ethereum 2.0

以太坊发展历程



Frontier

Homestead

Metropolis

Serenity

Ethereum 2.0

- 设计目标：
  - Sharding（分片）
  - Casper（PoS共识算法）
  - state rent
  - eWASM VM虚拟机
- 完全取代目前的以太坊（Ethereum 1.0），而将1.0作为其子链
- 分阶段进行，目前是信标链（Beacon）阶段

以太坊联合创始人Gavin Wood

- 以太坊联合创始人、CTO
- 计算机科学博士，科班大神
- 以太坊黄皮书作者，提出Solidity语言及EVM，C++版本以太坊钱包最早的作者
- 以太坊钱包Parity创始人
- 2015年离开以太坊
- 创办Polkadot波卡
- 参考文献： ĐApps: What Web 3.0 Looks Like （https://gavwood.com/dappsweb3.html）

Node 区块链加速器

The DAO事件回顾

The DAO事件与以太坊的硬分叉

- The DAO项目由 Slock.it 团队发起，2016年4月30日开始众筹，一个月募资1150万个ETH（当时价值1.5亿美元），占当时ETH总量约15%（投资者包括以太坊基金会），是当时有史以来融资最多的区块链项目
- 由于The DAO的智能合约设计缺陷，黑客成功攻击，至6月18日，已窃取超过360万个以太币
- 6月17日，Vitalik提出软件分叉方案，更新以太坊代码，使被盗的币永久封存。但需要51%以上算力支持
- 黑客认为自己的做法是合法的，而软分叉的做法不合法，并提出了要拿100万ETH奖励不支持软分叉的矿工，甚至有可能起诉“违约”的矿工或以太坊基金会
- 硬分叉方案：重写规则，让被盗的ETH回到原归属地址
- 两难：要么接受损失，维持约定；要么追回损失，更改约定（有违去中心化、不可篡改等设计初衷，开了个坏头）
- 7月20日，硬分叉实现，造成了以太坊分叉为ETH与ETC两条链，分道扬镳， 各自代表不同的社区共识（及利益）
- 目前ETH市值250亿，ETC市值10亿

The DAO事件与以太坊的硬分叉

- 至今仍充满争议，也引发人们对去中心化的巨大的思考
- 技术上也有悖论：
  - 世界上不存在没有漏洞、绝对安全的代码，如何基于共识去升级修补bug?
  - 软件的需求本身就是可变的，无法迭代式开发升级，大大限制了适用范围
- 后续仍有多个ICO项目因智能合约代码不安全，导致丢币事件屡次发生
- 此后Bitcoin也出现了硬分叉，经过开发者社区、矿工、持币者、矿机厂商等多方博弈，分为BTC和BCH
- 比特币与以太坊一个区别：中本聪和V神的区别

Node 区块链加速器

3.6
以太坊的应用开发

以太坊的应用开发起步

- 主要开发语言：Solidity，语法类似JavaScript，用于开发在EVM上执行的智能合约，以编译的方式生成EVM虚拟机代码
- 一个合约由一组代码（合约的函数）和数据（合约的状态）组成。合约位于以太坊区块链上的一个特殊地址（EOA账号地址）
- Browser-solidity （Remix）：基于浏览器的Solidity合约编译器 http://remix.ethereum.org/
- 编译合约后，会生成合约ABI和bytecode字节码。 ABI是合约接口的JSON表示，包括变量，事件和可以调用的方法；字节码是合约编译后的指令代码，可以在EVM上执行
- 其他用到的工具：如 Truffle做单元测试、Ganache便于在本机跑起来以太坊

Node 区块链加速器

3.7
EOS的创新

EOS简介

- Daniel Larimer（网名BM）发起的项目
- 致力于改变以太坊的性能、吞吐量问题，号称百万TPS（每秒处理交易量），实际目前达到几千级别（对比：比特币7、以太坊十几）
- 采用DPoS，类似议会选举制，21个“Block Producer”（国内称为“超级节点”）维护记账权
- 2017年发起，2018年6月启动主网上线
- BlockOne公司募资42亿美金，以及过度宣传，招致巨大争议
- 决策效率较高，由于新型激励机制的设定，社群活力较高

Node 区块链加速器

课后作业

课后作业（四选二）

1. 你认为以太坊上还能干什么？
2. 以太坊能全面替代目前的客户端/服务器模式吗？
3. The DAO事件中，如果你是V神，你会怎么做
4. 你认为有什么共识算法能取代PoW的挖矿机制吗？为什么？

Node 区块链加速器

扩展阅读

参考资料（本次课）

以太坊白皮书「Ethereum: A Next Generation Smart Contract & Decentralized Application Platform」

Smart Contracts: Building Blocks for Digital Markets – by Nick Szabo
http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

以太猫技术总监亲叙踩坑史: 为什么渐进式去中心化才是区块链的希望?
https://cloud.tencent.com/developer/article/1401564

Fomo3D游戏解读
https://mp.weixin.qq.com/s/Fhvba4MRB1sa7cg_JrK71A

区块链游戏，能否撼动腾讯和网易霸主地位?
http://www.8btc.com/gameblockchain

刘昌用：比特币扩容之争始末
https://www.jianshu.com/p/59dd742badd0

参考资料（增加中）

《浪潮之巅（第4版）》（吴军）

《信息系统的发展与创新》（蔡希尧）

《科技想要什么》（凯文·凯利）

《黑客帝国三部曲》

《Mastering Bitcoin（精通比特币）（第二版）》（Andreas M. Antonopoulos 等）

《密码工程实践指南》（ Steve Burnett 等）

《为什么我们的钱变薄了》（罗斯巴德）

《人类简史》（尤瓦尔·赫拉利）

《Mastering Ethereum（精通以太坊）》（Andreas M. Antonopoulos 等）

Node 区块链加速器