以太坊的由来：

* 介绍V神
  + 从小在计算机方面就展现出超过同龄人的天赋
    - 小学3年级就显现出了他在数学计算上过人的天赋，老师们发现这个小男孩可以用同龄人的两倍速进行三位数的心算，这让Vitalik轻松进入了学校专门为天才学生开设的“天才少年班”。
    - 10岁时，第一次接触到电脑。而他对电脑的初体验是[办公软件microsoft](https://cloud.tencent.com/developer/information/%E5%8A%9E%E5%85%AC%E8%BD%AF%E4%BB%B6microsoft) Excel。10岁正是小男生沉迷游戏的年龄，在大多数小男孩还坐在地毯上，玩火车模型，或在游乐园里奔跑追逐之时，当时也热衷于打游戏的V神却开始编程制作小游戏。
  + 接触比特币
    - 2011年 3 月开始，Vitalik成为了一名比特币行业的撰稿人：他在互联网上结识了正在建立《比特币周刊》（Bitcoin Weekly）的Kiba，Kiba为 Vitalik提供每篇文章5个比特币（当时价值3.5美元）的稿费，这也是他当时获得比特币的来源。钱虽少，但Vitalik却乐此不疲地投稿，后来因为比特币在当时仍缺乏主流媒体的关注，《周刊》最终还是逃不过关站休刊的命运。不过，在《比特币周刊》写稿的这段时间里，Vitalik积累了大量的关于比特币的知识和第一手资料。他也因为撰写的文章，结交了很多同样对比特币感兴趣的朋友，通过互相交流，Vitalik得以对比特币和区块链技术进行更深入理解。
  + 以太坊的创建
    - 通过交流，构思比特币2.0，希望打造出一个通用的平台，让开发者可以在上面构建自己的区块链应用。（这个构思就是智能合约的前身）
    - 2013年末，19岁的V神回到了多伦多，很快写下了一篇白皮书，建议设计一种新的比特币，并在文中介绍了“以太坊”。这款“新的比特币”将基于通用的编程语言，可以用来创建各种各样的应用，比如社交、交易、游戏……
    - 随后在2014年初，开始以太坊的建置工作。同年7月份，以太坊众慕启动，用户可以用比特币来预购以太币。兑换比例是：1个比特币兑换2000个以太币，按照当时每个比特币600美元的价格，一个以太币价值0.3美元。结果，此次众筹造成巨大轰动，12小时内募集超过3500个比特币；为期42天众筹，共计募得当时价值1840万美元的3万1千枚比特币。
    - 智能合约是以太坊吸引追随者的一大卖点，其通用性和可塑性让开发者们趋之若鹜。正是以太坊的智能合约，让众人对它背后的区块链技术产生了浓厚兴趣。
  + 如果说中本聪是区块链的创世者，那么如今才24岁的Vitalik则是一手将区块链推上了新的高峰，开启了区块链2.0时代。
* 以太坊的过去：
  + 历史路线图：
    - 前沿

前沿阶段始于2015年7月30日，该阶段用途是：将挖矿和交易所交易运行起来，建立一个让人们可以在里面测试分布式应用（DApps）的应用。

* + - 家园

次年3月14日，以太坊发布Homestead（家园），与前沿相比，家园没有复杂的技术性变革，只为以太坊提供了简单的图形界面的钱包，其中，易用性得到改善，普通用户也可以方便地体验和使用以太坊。

* + 历史大事件
    - The DAO事件
      * 什么是The DAO？

The DAO项目是区块链物联网公司Slock.it发起的一个众筹项目。原本该公司只想采用DAO（去中心化自治）来运作自己的系统Universal Sharing Network (USN)。后来发现这个机制也适合其他项目，因此决定创建The DAO，意为“DAO之母”。

* + - * 攻击细节

the DAO社区的每一位成员都可以利用自己手中的DAO进行投票，那么就会有一个问题，持有DAO数量越多，投票的占比就越大，会让投资决策出现偏颇，导致基金运行亏损。

所以the DAO就设计了一个“子DAO”的机制，你可以申请创建一个子DAO，审查通过后你的DAO就可以通过代码自动打入子DAO，从总资金池中剥离出来，而攻击漏洞也由此开始。

正常情况下你的DAO打入子DAO后就会从总的资金池中删除掉，但是看下图这行代码，里面的withdrawRewardFor是将钱从总dao打到你的子dao合约，注意前面提到的fallback函数，发送金额到你子dao合约时会触发fallback函数，但是如果你特别写了fallback是再调用总dao的withdrawRewardFor呢？代码会重新运行withdrawRewardFor再给你打钱，而扣钱的代码就永远不会运行到，如果你想，可以将总资金池中的DAO全部转空。

攻击者组合了2个漏洞，第一个漏洞是递归调用splitDAO函数，在第一次被合法调用后，会再次非法调用自己的DAO；第二个漏洞是DAO资产分离后避免从总资金池中销毁，攻击者在递归调用结束前将自己的DAO资产转移到了其他账户，就可以避免这部分DAO资产被销毁。

* + - * 后续影响

硬分叉之后，被盗的币找回来了，同时以太坊分为了两个链，一条为原链（ETC），一条为新的分叉链（ETH），也就有了现在的ETC（以太经典）和ETH（以太币）两种TOKEN，分别代表新旧社区的共识和价值观。

对于the DAO来说，这次事件无疑意味着项目的终结，甚至直接关联到2017年7月，美国证券交易委员会发布报告时提出，DAO提供和出售的代币是证券，因此受联邦证券法的约束，DAO违反了联邦证券法，所有的投资者也违法了。

* + - 以太猫网络拥堵
      * 什么是以太猫?



* + - * 以太猫带来的问题

数字猫交易游戏就已经变得十分受欢迎，但是因为CryptoKitties太火了！这也造成了以太坊网络拥堵，使交易速度变得缓慢。以太坊网络拥堵已经达到了前所未有的程度，30,000笔交易受到阻塞，正在等待处理。

CryptoKitties暴露了以太坊的一些问题。以太坊之前引以为傲的特性是，相比比特币，交易速度更快，手续费更低。但是仅仅是一个养猫游戏就让以太坊的转账网络拥堵，这实在让人大跌眼镜，进而产生对以太坊能否承担起更大额更实际智能合约应用的怀疑。

* + - Fomo3D事件
      * 什么是Fomo3D？

简单来说，Fomo3D是一个部署在以太坊网络上的资金盘游戏。简单说一下Fomo3D的游戏规则：

1. 一局游戏开始,系统自动按24小时开始倒计时。
2. 玩家可以花eth买入一个或者多个key，key就是分红权,key越多，得到的分红越多。
3. 只要有人成功购入key时，游戏倒计时便会被重置，即重新从24小时开始倒计时。
4. 玩家购买key所花费的eth会充入奖金池，之前买入过key的玩家会从奖金池获得分红。
5. 随着游戏的进行，key的价格会越来越高，购买一个key所需的eth会变多。
6. 没人购买key游戏倒计时便不会被重置，24小时倒数完毕，游戏结束。
7. 游戏结束，最后一个购买key的玩家为最终获胜者，其赢得资金池里48%的ETH。
8. 资金池里的ETH 48%分配给获胜者， 2%分配给社区基金会，剩余的50%按照四种团队模式进行分配.
   * + - 通过拥堵以太坊获取FOMO3D



* 以太坊的现在：
  + 大都会：拜占庭

大都会”又分为两个小阶段：“拜占庭”与“君士坦丁堡”。“拜占庭是第一阶段，已经在2017年10月完成”.。拜占庭升级引入了八项以太坊改进提案 (EIP)，且所有这些提案都于 2017 年 10 月在以太坊区块高度达到4,370,000 时生效。拜占庭升级的一个关键就是延迟难度炸弹，同时将区块奖励从 5 ETH 减少为 3 ETH。

* + 大都会：君士坦丁堡

以太坊此次以君士坦丁堡命名的硬分叉升级，经历了一波“三折”，动荡不止。

* + - 一波三折的以太坊升级
      * “一折”

2018年9月15日，以太坊核心开发者决定，将于10月9日在测试网络Ropsten上部署以太坊君士坦丁堡升级。

10月5日，由于升级版本中发现漏洞，升级经历“第一折”：被推迟至10月13日。

* + - * “二折”

时间转眼就到了10月13日，预期中的君士坦丁堡升级却未被如期激活。这次未被激活，并未有明确公告。分析人士认为，可能是升级中的EIP1234提案（出块奖励从3ETH降至2ETH，并将难度炸弹推迟12个月），遭到矿工抵制，没有足够的节点升级软件导致硬分叉升级版本未被激活。

以太坊网络升级经历“第二折”。

2018年12月7日，以太坊核心开发者召开电话会议，决定：将于主网区块高度7080000处（预计北京时间2019年1月16日）激活君士坦丁堡硬分叉升级。

* + - * “三折”

以太坊网络升级的“第三折”，在距离约定的升级版本激活时间数个小时之际到来。16日凌晨，安全审计公司ChainSecurity发布报告，称发现君士坦丁堡升级代码（EIP1283）存在漏洞，可能会导致“重入攻击”。

由于事发突然，出于谨慎考虑，以太坊官方宣布再次推迟网络升级时间。2019年1月18日，以太坊核心开发者再次召开电话会议讨论君士坦丁堡升级的相关问题，会议决定，将君士坦丁堡升级延期在区块高度7280000处激活。

历史上的君士坦丁堡同样也是经历了一波“三折”。

* + - 一波“三折”的君士坦丁堡（君士坦丁堡，一个历史上数次易主的城市）
      * 第四次十字军东征，君士坦丁堡被攻破，拉丁帝国建立；
      * 五十年后，拜占庭帝国光复君士坦丁堡；
      * 又过了数百年，奥斯曼帝国攻陷君士坦丁堡，拜占庭帝国覆灭。

V 神是俄罗斯人，而沙皇在历史上继承了拜占庭帝国接力棒，所以V神用拜占庭和君士坦丁堡作为两次网络升级的代号。公元 1453 年，君士坦丁堡被奥斯曼帝国攻陷，昭示拜占庭帝国灭亡，君士坦丁堡改名伊斯坦布尔。而下一次的以太坊硬分叉正巧被命名为伊斯坦布尔。

* + 大都会：伊斯坦布尔：

当前，以太坊团队目前正准备迎接下一次硬分叉升级--Istanbul(伊斯坦布尔)，这将会在大约八个月后进行。有报道称，伊斯坦布尔升级可能会包括为之前为君士坦丁堡升级提出的 EIP 提案，且提交针对伊斯坦布尔升级的 EIP的截止日期定于 2019 年 5 月。但是，预计我们将于 2019 年 7 月份在所有以太坊客户端上看到兼容于伊斯坦布尔升级的软件实现，且预计 2019 年 8 月份是以太坊测试网升级的截止日期。最终，预计伊斯坦布尔升级将在 2019 年 10 月份在以太坊主网中激活。

* 以太坊的未来：

宁静：

作为以太坊完整发展路线的最后阶段，“宁静”阶段意味着以太坊将完全抛弃PoW机制，转变至Casper PoS机制，届时也标志着以太坊将脱胎换骨，开始正式步入2.0时代。这将是以太坊甚至是区块链行业发展的一个重要节点，在PoS共识机制下，以太坊的社区治理、性能以及整个系统都将全面升级；再进一步，未来Sharding、EWASM的加入将会使以太坊性能大幅升级。然而如果“宁静”阶段能够在明年第一季度问世，以太坊完全转至PoS公式及之后，这也意味着，留给以太坊矿工们的时间或许不多了。Casper共识以及以太坊的分片将在后续章节中进行进一步的探索。