区块链分叉小史 —— 比特币篇

Author: Javierlev

Email: shenpanzhimao@gmail.com

前言

最近比特币现金(BCH)分叉把币圈搅得人心惶惶，各种主流数字货币纷纷跳水，币价争先恐后地往下跌，矿工不干了，把矿机砸了卖废品；韭菜绝望了，纷纷走上拥挤的天台。比特币现金(BCH)这个分叉于比特币(BTC)的加密货币，其实还是比特币早期就已经独立出来的儿子，在BCH之后，还有各种加密货币也从比特币分叉出来，但是命运各不相同。且在BCH从比特币分叉出来之前，还有一些隐秘的分叉未公诸于世。笔者在研究共识安全的闲余，来扒一扒区块链世界的各种分叉。本篇先从比特币的分叉史讲起，后续还有其他数字货币的精彩续集。

穿越必备小知识

既然要去探索分叉的历史，那么掌握一些分叉的知识是有很有必要的。否则，即使是重大历史事件就在你眼前发生，你也是面不改色，直接忽略。

什么是分叉

想象一条铁路，一直往前延伸。突然，在前方有一个岔路，铁路一分为二，向两个完全不同的方向延伸。 在比特币网络中，当两个新的区块同时生成的时候，这就形成了一个分叉。但是这个分叉还是可以撤回的，不是既定的事实，所以这时候还没有真正分叉。

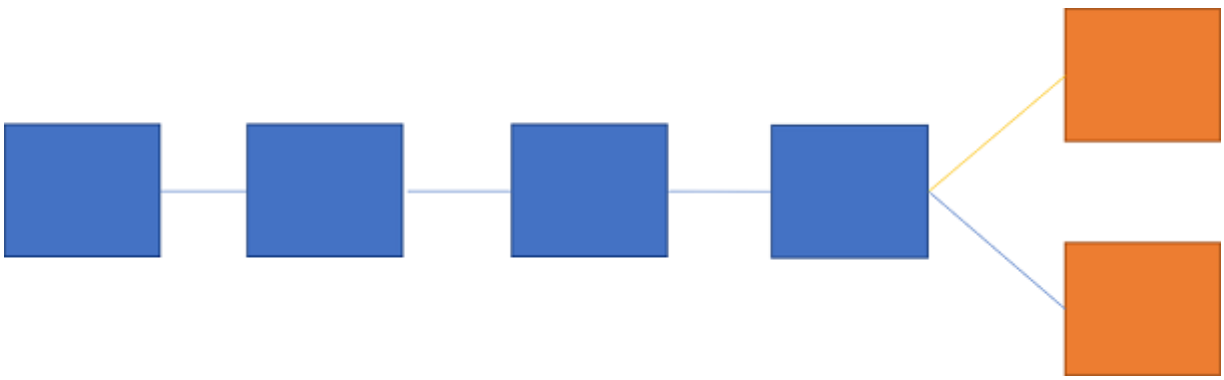


图1 分叉出现

真正的分叉叫做硬分叉，硬分叉就像比特币现金(BCH)分叉于比特币(BTC),两条链完全是不同链了，其币价也是不同的。

软分叉和硬分叉

分叉一定是坏的吗？ 不然不然，虽然BCH的分叉造成了币圈动荡，人心惶惶，但是分叉也是有好的。分叉还是一种改进区块链的升级方法。比如中本聪当初设计比特币的时候规定区块大小为最大为1MB，随着使用的人越来越多，有人提议把区块大小改大，这就需要通过软分叉来实现。具体就是在打包新的区块加入新的参数，规定在以后的生产区块中，如果没有发现2M的区块也允许加入到链中。通过这种方式，最大1M和2M的区块都存在于这条链上。这种升级法叫做软分叉，最终结果还是只出现一条链。

正方：不是说比特币有限吗？分叉之后比特币翻倍了！

反方：既然不同群体对比特币意见出现分歧，那么各取所需好了。

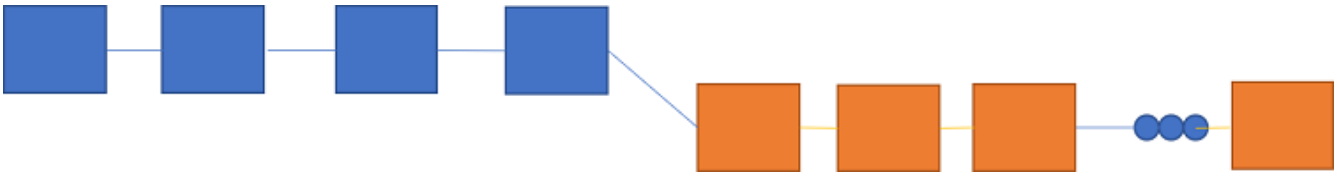


图2 软分叉

硬分叉的场景：新的区块中加入新的参数，新的链上拒绝接受没有新参数的区块，支持新链的矿工不断延伸新链(如图黄色区块)。支持原链的矿工同时延伸原链(蓝色区块),最终两条链分道扬镳。

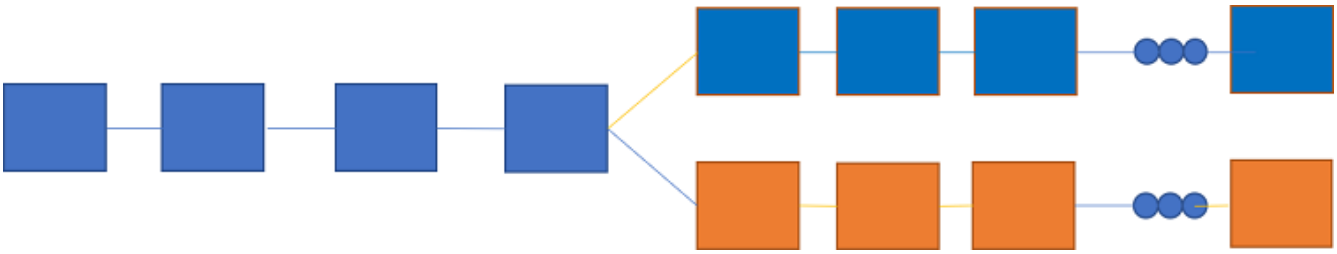


图3 硬分叉

PS:顺带一提,比特币现金BCH分叉的原因之一就是要不要升级区块的大小(软分叉)而导致了激进的硬分叉。

分叉正史

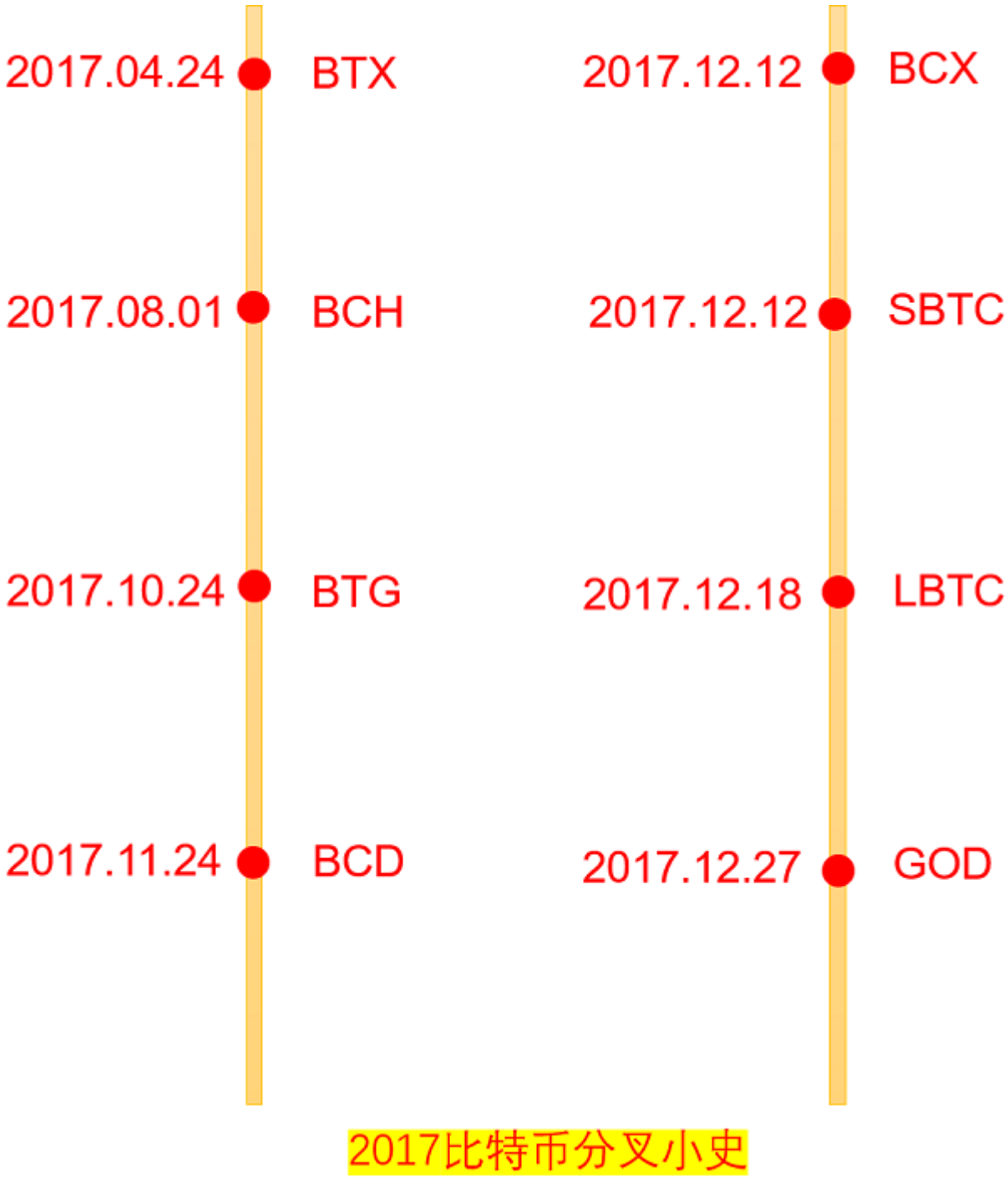


图4 分叉史

BTX

名称:

BitCore

分叉时间:

2017.4.24

分叉原因：

增大区块大小，缩减区块产生速度

小评：

据考证，这是比特币分叉史上开天辟地的第一次，也是必然的。区块链世界也需要不断升级，但，这只是一个开始。

BCH

名称：

比特币现金, Bitcoin Cash, BCH

分叉时间：

2017.8.1

分叉原因：

挖矿巨头比特币大陆旗下的矿池ViaBTC准备了一套硬分叉的体系，搅局比特币分叉方案BIP91。BIP91打算在区块中加入SegWit功能，并在之后的6个月内把底层区块链的区块大小升级至2M。而BCH决定支持大区块（将区块大小提升至8M），但不包含SegWit功能，是BitcoinABC方案产生的区块链资产。

小评：

本来是准备温和升级的软分叉，却成了激进的硬分叉，而且这次分叉的主角BitcoinABC在1年后的11月15日又将再次登上历史舞台

BTG

名称：

比特币黄金， Bitcoin Gold, BTG

分叉时间:

2017.10.24

分叉原因：

为了解决矿池中心化问题,引入一种新的共识算法`Equihash`，使得专门挖矿的ASIC矿机不具备优势。使挖矿时受限于内存而不是算力。

小评：

反对矿霸的币种，追求去中心化；虽是黄金，价格却低于现金。

BCD

名称：

比特币钻石，BitCoin Diamond，BCD

分叉时间：

2017.11.24

分叉原因：

提高隐私，在新区块上增加转账金额加密功能，使得交易转账金额不容窥探。使用segwit，使用闪电网络。

小评：

这是失败者东山再起的故事。由于Segwit2X(比特币分叉币SegWit硬分叉的币)失败，其运营团队又重新开发了比特币钻石来弥补缺憾。

BCX

名称：

比特无限，BitcoinX，BCX

分叉时间：

2017.12.12

分叉原因：

增加新特性：零知识证明以保护隐私，智能合约扩展功能，DPOS机制更加民主

小评：

宣称是未来的比特币，看起来是融合了ETH的智能合约,EOS的DdOS共识机制等元素，但是杂糅却使得本来的比特币血液更加庞杂，这是好还是坏，留给历史去评判。

SBTC

名称：

超级比特币，Super Bitcoin，SBTC

分叉时间：

2017.12.12

分叉原因：

对新功能进行实验

小评：

与比特币无限诞生于同一天，并且加入的新特性也有重合。不知道是不是模仿超级英雄，但是加入过多新特性也和比特无限同样贪心，不予置评

LBTC

名称：

闪电比特币, Lightning Bitcoin, LBTC

分叉时间：

2017.12.18

分叉原因：

修改共识机制为DPOS共识机制的区块链；增加智能合约

小评：

币如其名，追求闪电一般的交易速度。但是快不一定好，刚出来没多久就出现了一次技术分叉，性能与安全，闪电也需要找到一个平衡点。

GOD

名称：

比特上帝, Bitcoin God, GOD

分叉时间：

2017.12.27

分叉原因：

将数字货币应用于慈善场景，使用POS挖矿。

小评：

比特币上帝出现，不知道有没有比特币佛祖

分叉秘史

除了公布出来的比特币分叉之外，比特币历史上还有许多被隐藏的分叉。分叉真实发生，社区为了达到共识而选择让步，使得这些分叉回滚。

core开发组

比特币core开发组是维护比特币的技术核心团队。在比特币社区，core开发组成了在中本聪隐退之后的精神领袖。这个core开发组在2013年3月发布了带有bug的新版本比特币，新旧版本由于这个bug的存在而不能相互兼容，新版本将会拒绝旧版本的区块，导致了硬分叉。分叉持续了20多个区块，为了使比特币正常运行，社区达成回退版本的共识，一起退回了旧版本，分叉就此消失。

矿池

矿池是生产区块的主力军。但是矿池之间的分歧也会造成分叉。2015年7月，国内几大矿池连续挖出5个低版本的块，由于新旧不兼容，矿池达成共识，选择放弃到手的鸭子——区块，从而使比特币正常运行。

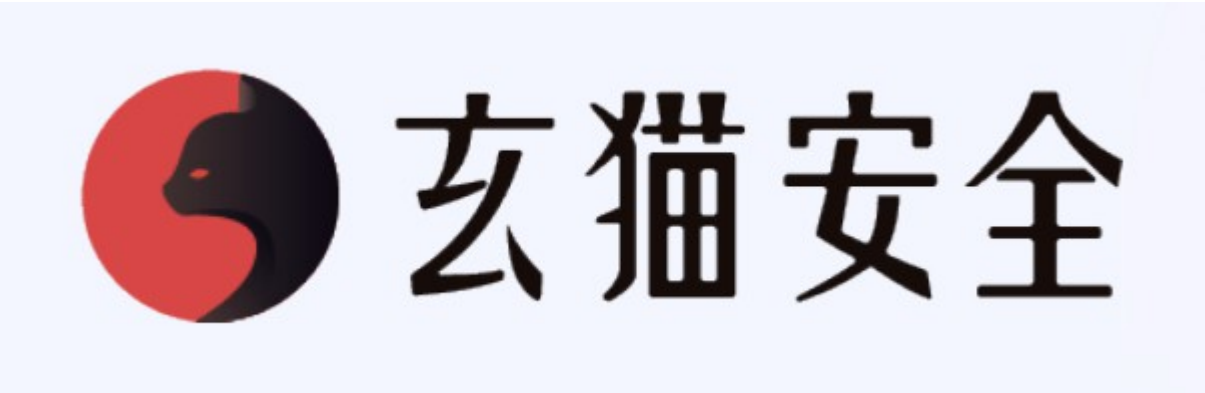
小结

本文简要介绍了分叉的概念与分类，同时扒了扒2017年比特币分叉出来的正史，提了提不为人知的秘史。无论是正史还是秘史，分叉都是由于共识不一致而导致的。 正史之中共识不一致主要集中在未来发展和应用的不一致，比如一拨人想要遵循中本聪的金科圣律，有一群人想要更加实用便捷的系统，大家都有技术，就通过在某个高度区块的高度分叉来单干。 秘史之中共识不一致主要由于开发时偶然产生的bug而导致新旧不兼容，这更像软件开发中版本不兼容导致的问题。 除此之外，攻击者还可以恶意制造分叉，统称为共识攻击。而针对不同共识机制，共识攻击所需要的条件也是不一样的。针对POW的共识攻击主要是51%攻击，所需要的是强大的算力，最近的BCH分叉的双方就是通过操控矿池的算力资源进行算力战，本质上也还是共识攻击。

后续

在分叉的时候，有一个必须注意的问题是重放攻击，分叉币如果没有做好防护措施，交易所会遭到重放攻击而损失资产。在算力战中，51%攻击又可以分为多种策略，资源+策略才能实施一场成功的共识攻击，这些在分叉小史——共识攻击篇将会讲到，下回见。

关于玄猫安全



玄猫区块链安全实验室专注区块链安全领域，致力于提供区块链行业最专业的安全解决方案，团队成员来自于百度、阿里、360等国际顶尖安全团队，已为数十家交易所、电子钱包、智能合约等提供基础安全建设、渗透测试、漏洞挖掘、应急响应等安全服务。

玄猫安全实验室提供专业权威的智能合约审计服务、区块链专项应用评估、区块链平台安全评估等多项服务。

商务合作：Lyon.chen@xuanmao.org