比特币的软件升级、分叉与暴涨

前言

最近几个月，扩容分叉成为比特币社区的核心议题。在持续争论中，社区已经分裂为几方力量，各方都提出了不同的方案。最终的扩容依然在实施过程当中，由矿工ViaBTC主导的BCC（Bitcoin Cash，彻底解除区块大小限制）硬分叉已经开始运行。未来11月的2M升级可能会激发新一轮的分叉。

这一话题主要散见于大量的新闻稿，技术问题、经济利益、权力斗争和理念差异纠缠在一起，缺乏一个完整详尽中立客观的史料性的综述，人们无法看到事情的真相、可能的选择和最终取舍与进展。故作者萌生了梳理事实、厘清脉络的考虑，本节将尽可能全面客观地回顾比特币社区在这一问题上的进展。

特别致谢两位从未谋面的朋友提供的帮助，帮我厘清了一些模糊和混乱的认识。因两人不愿具名，故此匿名感谢。

GitChat

升级一个全球计算机的分布式协作网络，绝不简单。更困难的在于，新升级版本需要跟旧版本在同一个区块链上工作。这涉及到巨大的利益、风险和未来的发展方向。

区块链跟其他软件最大的不同在于，区块链软件的升级中涉及到的新旧版本兼容更为重要和复杂，因为在一个去中心化网络中，节点很可能不会同步升级，这样会发生新旧版本同时产生出区块、而且互不兼容，这可能会导致区块分叉。区块分叉的后果之一是，每个区块的Coinbase会产生新币，这样网络中就出现了两种币。一般认为，硬分叉产生两套新币的过程会对整个生态系统带来混乱和负面影响。

最近两年比特币社区的争论围绕着两个焦点，第一，隔离验证，第二，区块扩容。隔离见证将签名数据移到区块结构外，可以优化数据结构，同时可以部分地对区块扩容。至于区块扩容，则是由于网络上的交易量越来越大，中本聪原来设定的1M区块大小限制已经达到，因此大量交易无法及时得到矿工确认，导致排队延时严重，网络拥堵无法得到缓解，未来通过硬分叉将区块大小改为2M或者更大已经迫在眉睫。

隔离验证

隔离验证Segregated Witness也被人们称为隔离见证。每一个比特币交易，其实可以分为两部份。第一部份是说明余额的进出，第二部份是用来证明这个交易的合法性 (主要是签名)。第一部份可称为“交易状态”，第二部份就是所谓的“见证”(witness)。一般用户只关心每个账户的余额，因此交易状态资料就已经足够。只有部份人(主要是矿工)才有必要取得交易见证。

中本聪设计比特币系统时，并没有把两部份数据分开处理，导致交易ID的计算混合了交易状态和见证。因为见证本身包括签名，而签名不可能对其自身进行签名，因此见证是在缺乏交易双方同意下任何人都可以改变的，造成所谓交易延展性(Malleability)。将签名放在交易结构中，由于签名的可塑性，使得交易也就有了可塑性。

也就是说，将签名数据放在交易数据中其实没有任何好处，反而增加了结构的复杂度和交易延展性的风险，显然是得不偿失的。在交易发出后，确认前的交易ID可以被任意更改，因此基于未确认交易的交易是绝对不安全的。在2014年曾有人利用此漏洞大规模攻击比特币网络。

比特币核心开发者Pieter Wuille 2015年12月於香港提出的隔离见证软分叉BIP141巧妙地彻底解决了这个问题。隔离验证，就是把原来的比特币交易中签名数据单独拿出来放到另一个叫 witness 的结构中，做到——交易是交易，签名是签名。

隔离验证带来的好处包括以下六点：

1. 通过软分叉增加最大区块容量。旧有节点根本看不到新的被隔离的验证，即使真实区块已超过1MB，它们仍会以为没有超过限制而接受区块。不扩容条件下SW可以提供约1.6-2MB的有效区块空间而没有任何硬分叉风险。

2. 保证只有发出交易的人才可以改变交易ID，任何其他第三方都不可以。如果是多重签名交易，就只有多名签署人同意才能改变交易ID。这可以保证一连串的未确认交易的有效性，是双向支付通道或闪电网络所必须的功能基础。有了双向支付通道或闪电网络，二人或多人之间就可以实际上进行无限次交易，而无需把大量小额交易放在区块链，大大降低区块对存储空间的需求。

3. 轻量钱包可以变得更轻量，因为它们无需再接收见证数据。

4. 可以大幅改善签名数据结构，为更强大的功能扩展打下了基础，如脚本语言升级。

5. 实行隔离见证後，当无效区块出现时就可以产生很简洁的欺诈证明，这会令进行简单交易验证 (SPV) 的轻量节点的安全性更接近全节点，可以令整个网络在较少的全节点下仍能运作。

6. 隔离验证将降低比特币交易费用。《精通比特币》的作者Andreas M. Antonopoulos曾撰文分析了这一点。隔离验证对交易费有两大影响。首先，隔离验证通过分离验证数据降低了交易的总体成本，并变相增加了比特币区块链的容量。其次，隔离验证可能会通过交易费降低的激励，纠正交易的UTXO集结构，进一步降低交易对网络所造成的负担。每笔添加到比特币网络的交易，影响了节点的四个资源消耗：磁盘空间、CPU、网络带宽和内存。比特币交易的数据结构的优化，能够改善资源的消耗和占用。

当然，隔离验证也带来了一些缺点和潜在风险。首先，现有钱包软件都需要升级以兼容新的交易格式。其次，隔离见证在全网应用，代表着4倍多的带宽占用。带宽占用将在未来扩容区块大小时更显得重要。当然还有一些其他的潜在问题。

隔离验证其实是对之前不太合理的比特币交易结构的优化，开发者们试图用一种影响尽可能小的、尽可能向下兼容的、“软分叉”的方式来实现，这种改进本身（就像是“压缩格

GitChat

式的公钥”一样）是非常合理的，与区块大小之争并无直接的关系。

Segwit带来的最明显的好处是：使得闪电网络能够得以顺利应用。2015年Joseph Poon和Tadge Dryja两位开发者首次在白皮书中提到了这一概念。这是一种种支付通道的想法，能够将小额交易发生在比特币区块链以外，能够促进比特币的交易吞吐量达到每秒百万笔。

一些比特币企业和用户仍然认为隔离见证是错误的选择，他们坚信这一点，并因此分叉了比特币区块链，将这种新链命名为比特现金（BCC，移除了隔离见证）。Bitcoin Cash矿工在8月1号UTC时间12:37，区块高度478558开始了分叉的第一步。6个小时之后，Viabtc挖出了第一个Bitcoin Cash块（#478559），接下来的第三个块也是由Viabtc矿池挖出的。第一个Bitcoin Cash区块大小为1915175字节，即1.9MB，其中包含了6985笔交易。这一容量高于比特币1MB的限制，交易吞吐量也多出了约3000笔。Viabtc还在区块数据中写道“欢迎来到这个世界”。

BIP百家争鸣时间线

bip141 隔离验证的最初BIP，详细描述了一个叫 “witness” 的新数据结构，脚本和签名等数据被移动到了这个新结构中，同时介绍了隔离验证如何做到的向下兼容等；2016年11月推出的BIP 141是激活SegWit的原始计划。

GitChat

bip142 讲述了隔离验证的新的地址格式；

bip143 举例描述了隔离验证交易签名的验证方式；

bip144 讲述了如何在保持向下兼容的情况下节点间通报支持隔离验证的情况及传播和请求验证数据的方式；

BIP 148：2017年3月发布，BIP 148被开发为通过用户激活的软分叉（UASF），强制推动停滞的BIP 141。

BIP91：Hilliard提出了一个稍显复杂但巧妙的解决方案，可以使一切都能互相兼容：Bitcoin Core开发团队提出的隔离见证激活，BIP148 UASF和纽约共识激活机制。他的BIP91可以使比特币保持完整，至少在隔离见证激活的时候。只要大多数矿工在8月1日之前激活BIP91，所有比特币节点都应该仍然是同一网络的一部分。

作为SegWit2X扩展计划的第一部分，BIP91做了两件事：

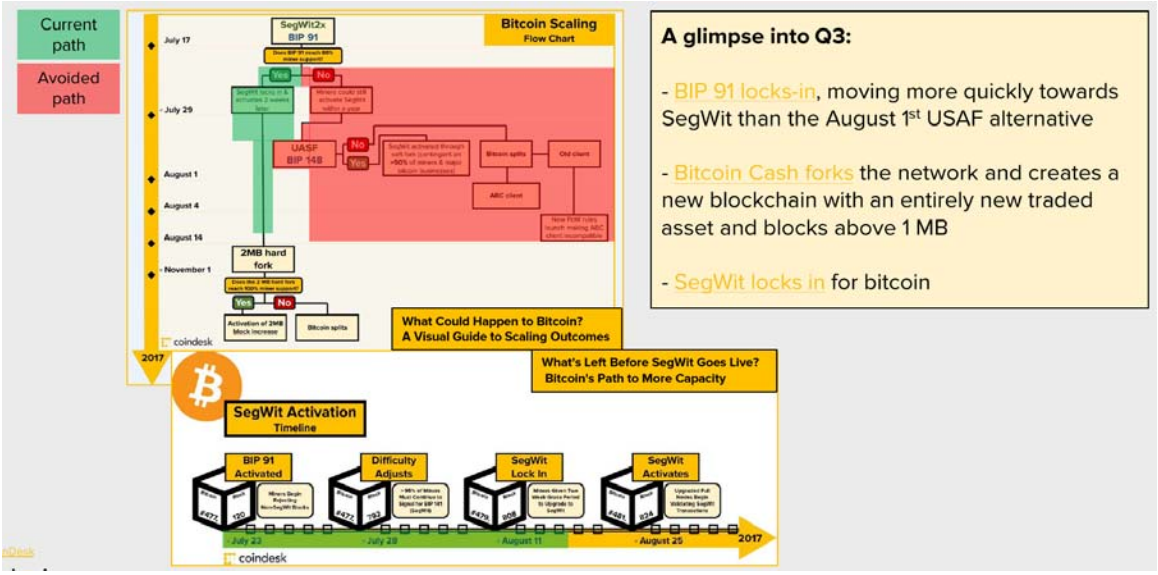
1. 它使网络更容易激活隔离见证(SegWit)。隔离见证是一个向后兼容的升级，修复了比特币交易信息的延展性，并为诸如闪电网络这样的外链解决方案扫清了道路。

2. 如果在7月31日之前启动，BIP91将取代BIP 148。BIP148这一提议有可能导致网络分裂。最终BIP91取得成功。

作为SegWit2x扩展计划的第一部分，BIP91做了两件事：

1. 它使网络更容易激活隔离见证(SegWit)。隔离见证是一个向后兼容的升级，修复了比特币交易信息的延展性，并为诸如闪电网络这样的外链解决方案扫清了道路。

2. 如果在7月31日之前启动，BIP91将取代BIP 148。BIP148这一提议有可能导致网络分裂。最终BIP91取得成功。



简单来说，现在社区有三股力量：

1. 已经分叉成功的BCC（也有些人认为BCC不是分叉币而是山寨币）；BCC是用户激活硬分叉（UAHF）带来的结果。UAHF首次亮相在比特大陆（Bitmain）针对BIP 148用户激活软分叉（UASF）提出的分裂应急预案中。BCC将会移除隔离见证（SegWit）的部分，默认区块容量是8MB。至少在8MB的区块大小中，发动垃圾交易攻击的成本是很高的。

2. Bitcoin Core团队（极端保守，不愿实施任何有风险的硬分叉）、Bitcoin Core的政策清晰，且一贯如此：不会进行有争议的硬分叉。Core团队的优势：Core团队拥有很多开发者，不过流程很慢。流程较慢通常产生的错误也会更少，不过会提高错误的成本，因为较慢的流程同样适用于错误的修正。

3. Segwit2X（协助推动Segwit实施并积极推进2M硬分叉扩容）。

以下是重要事件的时间线：

2017年2月，开发者Shaolinfry在提出新构想：用户激活软分叉或UASF。用户激活软分叉（UASF）。与哈希率激活不同，用户激活软分叉将使用“指定日激活”，其中节点会在将来的一个预定时间开始强制执行新规则。“只要UASF被大多数的经济参与者执行，这应该会迫使大多数矿工遵循（或激活）软分叉。

2017-4-6 比特币测试网络挖出3.7MB区块，隔离见证增加区块大小被证实。测试网络上还发现了一个1.7MB的区块，其中包含了超过8，000笔交易。

2017-4-9 莱特币创始人兼Coinbase工程主管李启威（Charlie Lee）称SegWit可实现比特币与莱特币互操作，降低比特币手续费。

2017-4-10 ASICBOOST闹剧，BU支持者比特大陆（Bitmain）在中国持有ASICBOOST的专利。可能有小部分矿工部署了ASICBOOSt而获得了某种挖矿优势。社区对BU和Bitmain的信心下降。

2017-4-11 开发者提出UASF用户激活软分叉BIP148，避开矿工的投票过程。UASF要想激活就需要获得来自“经济大多数”(如交易所，钱包和其他比特币经济参与者)的明确支持。

2017-4-27 莱特币的SW算力投票已达到激活阈值75%，两周后锁定再两周后激活。（http://litecoin-segwit.info/ ）主要动因是矿池BW.com投票支持。5月10日，莱特币正式激活SW。

5月12日，比特币勒索病毒WannaCry全球肆虐。

5月23日，Segwit2X（Segwit then 2M fork）即纽约共识NYA出台。

7月12日，Core团队警告UASF（BIP148）可能引起网络分裂。

Core发了一则措辞严厉的公告《警告：可能的网络分裂》，称7月31日UASF（BIP148）软分叉发起后，有可能出现比特币分叉，并且BIP148分叉在得到足够算力支持后，有可能覆盖重写主链，因此用户收到的币，不管是经过多少个确认，最后都可能从钱包中消失，比特币有可能分裂成两条链。这一警告引起了极大的恐慌，币价应声大跌，最低崩盘至12900，几乎从前阶段高点跌掉了了40%。事后来看，Core的这一警告是无端的、荒唐的，隐瞒了Segwit2X已经兼容BIP148因而BIP148已不可能发生的事实，有故意夸大其词造成恐慌的嫌疑。
可能是受此暴跌影响，矿工们开始积极考虑如何避免USAF，积极信号支持BIP91。结果，在Segwit2X开始投票锁定后，币价迅速上涨，恢复到了19000元，并最终创出了新高32000元左右。

GitChat

7月18日，Segwit2X激活代码BTC1正式发布。支持BIP91的矿工增加，BIP91整合了Segwit2X和BIP148。

7月21日，BIP91正式锁定。

7月22日，BIP91激活，不使用隔离见证(BIP141)的区块将被拒绝。BIP148正式被取代。这促成了BIP 141的锁定以及Segwit的最终激活。

7月28日，BIP141投票开始（95%区块支持阈值），获得接近99%的算力支持。

8月1日，BCC诞生，算是比特币社区的一次硬分叉（UAHF）。比特币价格略有波动，但立即恢复，市场未见恐慌。意味着社区已经接受了分叉现状，并认为BCC不会对比特币产生冲击。

8-10 Core团队称新版Bitcoin Core 0.15.0不支持SegWit2x节点，正式宣告与Segwit2X分道扬镳。鉴于隔离见证（SegWit）激活已经锁定，BIP148也生效了，新版客户端将会自动切断任何运行SegWit2X分叉节点。看起来Bitcoin Core开发者想要防止11月硬分叉再给比特币用户造成重大影响。

同时，segwit2X团队称，Segwit2x提案得到了大量矿工的支持。据GitHub上公告，预计在11月份，全网90%的比特币算力会开始切换到这个新的分叉链。segwit2X的客户端也将不与core兼容。

8月11日Segwit锁定。

8月中旬，Segwit2x工作组成员Jean-Pierre Rupp公布了该团队制定的2MB硬分叉计划。计划于2017年11月，也就是在隔离见证激活的约90天之后，比特币矿工将会生成1MB到2MB大小之间的区块，旨在实现网络扩容。目前，预计有超过90%的比特币网络算力将会在这一大区块上参与挖矿。2MB升级是在香港圆桌共识中首次提出的，在今年的Consensus大会上，这一升级通过纽约共识（NYA）得到进一步强化。这两项共识都包含了先激活隔离见证，后实现1MB到2MB扩容的内容。

8月18日，Bitcoin Core发表了《Correcting misinformation on Segwit2x and btc1》一文，重申了对Segwit2X和btc1的质疑和不支持。

8月24日，Segwit（BIP141）正式激活。区块高度481,824， 由BTCC矿池挖到。

9月1日，F2Pool称改变想法不再支持Segwit2X，且并未运行BTC1。

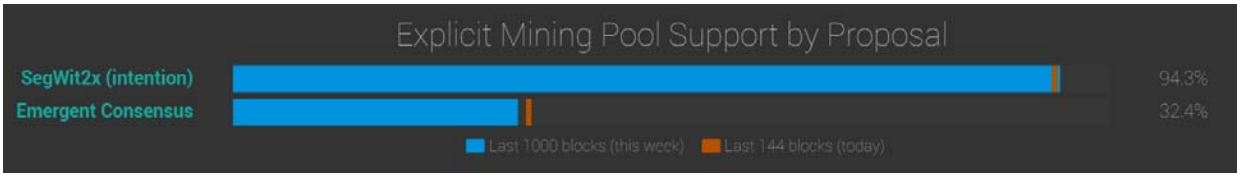
9月14日，Bitcoin Core公布了0.15.0代码。界面给出了更多估计矿工费的选项，增加了对多个钱包的支持。

GitChat

> Segwit2X硬分叉计划：
>
> SegWit2x解决方案最初由Rootstock首席科学家Sergio Demian Lerner提出。至此之后，比特币行业的很多矿工和企业在纽约Consensus 2017大会上签署了一项协议。SegWit2x的代码目前正在由比特币开发者Jeff Garzik领导的SegWit2x研究团队来进行开发。具体分叉计划为：
>
> 在SegWit在SegWit2X客户端激活之后的第12,960个区块，SegWit2X的2MB硬分叉将自动在所有运行SegWit2X的节点上激活。如果某一个硬分叉在激活时获得75%+的算力支持，这个分叉将强迫其他所有网络节点升级到SegWit2X（或兼容SegWit2X），否则将被从这个分叉网络中踢出。区块494784将成为硬分叉点。（11月18-19日前后）

当前网络进展

（时间：2017-9-30）
BIP 141 Segregated Witness 已经激活；Segwit2X(intention) 获得 94% 支持（last 1000blocks）；（数据来源：Coin.dance）



节点实际使用的软件版本情况：9-30数据（数据来源：Coin.dance）

上图显示，73%的节点依然使用BItcoin Core软件，8%的节点使用了Bitcoin ABC（Bitcoin Cash），使用BTC1（即Segwit2X工作组的软件版本）的节点仅有204个，占比仅为2.2%。简单总结现状就是，大部分人实际使用的是Bitcoin Core的软件，但是口头支持Segwi2X硬分叉。目前状况，似乎还没有发展到矿工们必须选择一方抛弃另一方的最后关头。

GitChat

未来，到底是拒绝扩容的Core取胜，还是稳健扩容的2X取胜？

也许，11月的硬分叉会最终给出答案。（正文完）

小词典——分叉后果之重放攻击

重放攻击：传统术语“重放攻击”：指的是身份欺诈。在维基百科上定义很清晰，如下：

假设Alice向Bob认证自己。Bob要求她提供密码作为身份信息。同时，Eve窃听两人的通讯，并记录密码。在Alice和Bob完成通讯后，Eve联系Bob，假装自己为Alice，当Bob要求密码时，Eve将Alice的密码发出，Bob认可和自己通讯的人是Alice。

百度百科的解释与之类似，但更一般化：

> 重放攻击（Replay Attacks）又称重播攻击、回放攻击，指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。重放攻击可以由发起者，也可以由拦截并重发该数据的敌方进行。攻击者利用网络监听或者其他方式盗取认证凭据，之后再把它重新发给认证服务器。重放攻击在任何网络通过程中都可能发生，是计算机世界黑客常用的攻击方式之一。

在数字货币社区，重放攻击不是一种“攻击”，仅仅是硬分叉后产生的两条链，共享了同一条母链（地址、交易、算法、难度等），因此A链上合法的交易，在分叉的B链上也可能完全合法，因此可以在B链上重新广播一次。甚至发生将A链的币发送到了B链的地址的混乱情况。

比如，以太坊在192万区块高度发生了硬分叉，产生了两条链，分别称为ETH chain和ETC chain，上面的代币分别称为ETH和ETC。这两条链上的地址和私钥生产算法相同，交易格式也完全相同，导致在其中一条链上的交易在另一条链上很可能是完全合法的。所以你在其中一条链上发起的交易，就可以到另一条链上去重新广播，可能也会得到确认。这就是“重放攻击”。

本文首发于GitChat，未经授权不得转载，转载需与GitChat联系。

实录：《丹华：解析比特币的软件升级、分叉与暴涨》

发起一场Chat！