**目 录**

**[1. 什么是比特币分叉 1](#_Toc2358)**

**[2. 分叉的类型 2](#_Toc24061)**

**[2.1. 硬分叉 2](#_Toc15415)**

**[2.2. 软分叉 2](#_Toc26118)**

**[3. 比特币为什么会分叉？ 3](#_Toc19602)**

**[4. 比特币扩容之争 3](#_Toc6328)**

**[4.1. Bitcoin XT 3](#_Toc29142)**

**[4.2. Bitcoin Classic 4](#_Toc14075)**

**[4.3. BIP141+闪电网络 4](#_Toc6786)**

**[4.4. 香港共识 4](#_Toc10685)**

**[4.5. Bitcoin Unlimited 5](#_Toc5768)**

**[4.6. 纽约共识（Segwit2X） 5](#_Toc26849)**

**[4.7. UASF（用户激活软分叉） 5](#_Toc12053)**

**[4.8. UAHF（用户激活硬分叉） 5](#_Toc20078)**

**[5. 比特币的分叉 6](#_Toc23926)**

**[5.1. 非扩容分叉方案 6](#_Toc24657)**

**[5.1.1. BTG（比特黄金） 6](#_Toc8789)**

**[5.1.2. 比特钻石 6](#_Toc11581)**

**[5.1.3. 超级比特币 6](#_Toc18334)**

**[5.2. 近期分叉币种介绍 7](#_Toc32098)**

**[6. 相关技术原理 7](#_Toc27340)**

**[6.1. 增大区块容量 7](#_Toc24091)**

**[6.1.1. 区块头部 8](#_Toc23158)**

**[6.1.2. 交易的数据结构 9](#_Toc1983)**

**[6.1.3. 交易输入 9](#_Toc26951)**

**[6.1.4. 交易输出 11](#_Toc22323)**

**[6.2. 隔离见证： 12](#_Toc10706)**

**[7. 对交易所的风险 14](#_Toc8445)**

**[7.1. 重放攻击 14](#_Toc25050)**

**[8. BTC分叉交易所应对方案 14](#_Toc4569)**

**[9. 为应对分叉对交易所的建议 15](#_Toc14599)**

# **什么是比特币分叉**

比特币网络正常运行依赖于节点按一致的规则检验和收录区块，这种情况下即便偶尔同时有多个相同高度的正确的区块产生，也会按照最长链规则归集到一条链上。

但当比特币协议升级时，网络中会存在遵守不同的规则的旧节点和新节点时，就会存在区块链分叉且不能迅速回归同一链的可能，这种情况称之为分叉。

# **分叉的类型**

分叉主要分为软分叉和硬分叉：

* 1. **硬分叉**

当系统中出现了新版本的软件（或称协议），并且和前版本软件不能兼容，老节点无法接受新节点挖出的全部或部分区块（认为不合法），导致同时出现两条链。

分叉后，继续运行旧版软件的节点将发现新交易是无效的。因此为了切换到新链继续挖有效区块，所有网络节点必须升级为新规则。

当出现某种政治僵局，社区部分人坚持旧规则，就会出现问题。旧链的哈希率、网络算力将变得不合时宜。重要的是，旧链的数据和规则仍被看作具备价值，矿工当然希望继续挖矿，开发者也希望继续支持它。

* 1. **软分叉**

当系统中出现了新版本的软件（或称协议），并且和前版本软件不能兼容，新节点无法接受老节点挖出的全部或部分区块（认为不合法），只有一条链。

没升级的节点会继续将新交易视为有效的，然而未升级节点继续挖出的区块将被升级节点拒绝。因此软分叉执行成功需要网络的大部分算力，只要执行软分叉的算力不占有绝对的优势，无法使用追随最长链规则孤立掉不升级的算力打包的区块，那就会分裂。

# **比特币为什么会分叉？**

随着比特币的不断发展，使用比特币的人数和区块链上的交易越来越多，1M区块大小成为比特币发展瓶颈，导致了比特币网络拥堵问题日益严重，制约了比特币的发展。为了比特币更好的发展，比特币社区开始讨论修改比特币的协议和代码，突破比特币的1M区块上限，加快交易的速度。以这个初衷为出发，伴随着比特币商业化日趋严重后矿工与开发者之间利益与理想之间的博弈，以及开发人员之间技术理念的不同，造就了比特币长达几年的扩容讨论和如今的数次分叉。

# **比特币扩容之争**

对于比特币扩容，争论的双方主要有两个：矿工和开发人员。矿工出于利益的追求，想要获得更多的区块奖励和交易手续费，更偏向现实主义；开发人员的初衷是维护区块链去中心化的理念，更偏向理想主义，并且开发人员之间由于技术理念的不同也会有相应的争论。造就了持续几年的对于比特币扩容的讨论，出现了多种方案。

* 1. **Bitcoin XT**

2011 年，Gavin Andresen 被中本聪指定为比特币的首席开发者，之后 Gavin 又吸纳了多名技术人员加入开发者的团队，于是逐渐形成了我们今天看到的 core 开发组。

2015 年初，他提出将比特币区块一次性扩容至 20MB，在当时由于在中国这样的发展中国家的网络条件无法满足这么达的区块，因此这个提议没有在社区达成共识。2015 年底，20MB 扩容计划落空的 Gavin Andresen 联合开发者 Mike Hearn 提出了将区块大小调整至 8MB 的 Bitcoin XT 方案。

该方案 基于 BIP101 协议将起始块的上限设为 8MB，随着时间的推移，区块上限逐渐提高。 但这个方案同样没有获得开发组其他成员的认可。2016 年初 Gavin Andresen 被取消了比特币维护权，Mike Hearn 退出比特币社区。

* 1. **Bitcoin Classic**

该方案在2016年3月份，由前比特币基金董事Olivier Janssens，FinalHash 首席执行官Marshall Long和比特币矿工和开发人员Jonathan Toomim提出，他们 基于BIP109协议，延续了中本聪的思想，在他的代码库基础上将区块大小扩大到2MB。并获得Gavin Andresen和Jeff Garzik等开发者的支持。

该方案需要获得75%以上算力支持才能够被激活，激活之后28天才会发生硬分叉。但该方案遭到了BlockStream等区块链技术开发公司的反对。

* 1. **BIP141+闪电网络**

对于bitcoin classic方案，core团队持反对态度，他们希望 坚持主链区块1M 大小不变，因此提出采用隔离认证（segwit）+ 闪电网络的方案解决比特币交易拥堵的问题 。

* 1. **香港共识**

2016年 2月，Core开发者和矿工双方在香港数码港达成协议，实施BIP141（隔离见证）+ 硬分叉2M，并且限制矿工不能运行Bitcoin Classic。

但是由于Core团队参加会议的几个主要的开发人员回去后遭到其他开发者的反对，香港共识被迫中止。

* 1. **Bitcoin Unlimited**

该方案提出 不给单个区块设立上限，产生新区块后，由矿工通过“紧急共识”作出决策，决定区块大小 。但最终因为开发能力不足，出现几次Bug之后被迫停止。

* 1. **纽约共识（Segwit2X）**

今年5月，Barry Silbert旗下的数字货币集团（DCG）和包括大型矿池运营商比特大陆（Bitmian）在内的其它57家公司共同签署segwit2x扩容方案。该方案将隔离验证激活阈值设为80%，并以bit 4作为信号发送方式；在六个月内执行一次2 MB硬分叉扩容 。

* 1. **UASF（用户激活软分叉）**

Core开发组中的极端人员发起的一个的提BIP148，直接绕过矿工投票，改成8月1日直接激活隔离见证，这个被称为用户激活软分叉（UASF）。这个方案存在对比特币造成分裂并且存在重组的风险。

* 1. **UAHF（用户激活硬分叉）**

因为BIP148的软分叉方案对原链有重组的威胁（表现在于没有大多数算力的支持，会造成软分叉分裂。一旦分裂之后的链的增加速度超过原有链，那么根据最长机制原则势必有一天会放弃原有链，原有链分叉之后的区块数据将丢失），所以社区一些人提出了该方案，并获得了比特大陆算力的支持，该方案将区块大小提高到了8M。

# **比特币的分叉**

* 1. **非扩容分叉方案**

伴随着比特币扩容方案的讨论，一些方案也被更新到了最新的比特币客户端之中，比如Segwit2x、UASF、UAHF。一些方案分叉失败，比如UASF、Segwit2x，UAHF的分叉方案产生了分叉币BCH。

但是由于对比特币的信仰理念和商业利益之争，也有一些在扩容方案讨论之外的协议升级方案，这些方案初衷并非单单为了解决比特币的扩容问题，我称之为“非扩容分叉方案”。这些非扩容方案也造就了如今众多光怪陆离的比特币分叉。

* + 1. **BTG（比特黄金）**

此次分叉的策划者为LightningASIC的首席执行官廖翔。他认为如今的比特币深受挖矿中心化的困扰。比特币可以由ASIC开采集中算力进行开采，但只有少数人有权访问。此外，一些中国的大型公司占据了大部分挖矿的算力，这违反了完全去中心化的加密代币的理念。因此，廖翔及其团队进行了这次分叉，修改了比特币原本的挖矿算法，从SHA-256到EQUIHASH，使挖矿过程对现在的ASIC挖矿芯片不友好。

* + 1. **比特钻石**

海外EVEY团队和007团队联合退出的分叉方案，为解决比特币用户数量激增随之出现的隐私保护、转账手续费用过高、处理交易速度缓慢等问题。该方案会在预定的495866区块高度下，让比特币钻石矿工将使用新的工作验证算法开始创建区块，并且将发行的总量增加到比特币的10倍，即2.1枚比特钻石。

* + 1. **超级比特币**

李笑来发起的比特币分叉方案，该分叉方案为增加区块大小到8M，并加入了零知识证明、智能合约、支持闪电网络等新特性。预计在498888区块高度上进行分叉，SBTC总量发行2121万，其中21万是分叉预挖。

* 1. **近期分叉币种介绍**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 方案名称 | Sigwit2x | UAHF | 比特黄金 | 比特钻石 | 超级比特币 |
| 分叉类别 | 扩容分叉 | | 非扩容分叉 | | |
| 分叉类型 | 硬分叉 | 硬分叉 | 硬分叉 | 硬分叉 | 硬分叉 |
| 新代币 | bt1、bt2 | BCC | BTG | BTD | SBTC |
| 交易所 | Okex上有合约交易，后下架 | Bittrex、GateIO、CEX等 | GateIO、bleutrade | 暂无 | 暂无 |

# **相关技术原理**

目前主流的扩容方案主要为**增大区块容量**及**隔离见证**。

* 1. **增大区块容量**

目前比特币的区块容量大小为1M，比特币的交易信息都存储在区块当中，每一个数据区块记录了六个内容：神奇数、区块大小、数据区块头部信息、交易计数、交易详情。区块的组成结构如下：



所以增大区块大小，让一个单位里区块承载更多的交易，从而增加比特币每秒的承载交易数，成了很多人提出的解决方案。

区块详细组成如下：

* + 1. **区块头部**

数据区块头部结构中记录了：版本号、前一个区块的记录、Merkle树的根值、时间戳、目标特征值、随机数。区块头部的数据结构图如下：

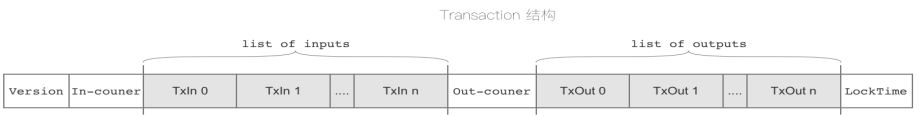
****

* + 1. **交易的数据结构**

交易的本质是一个包含交易发送方、接收方、资产转移等相关信息的数据结构，其数据结构如下表所示：

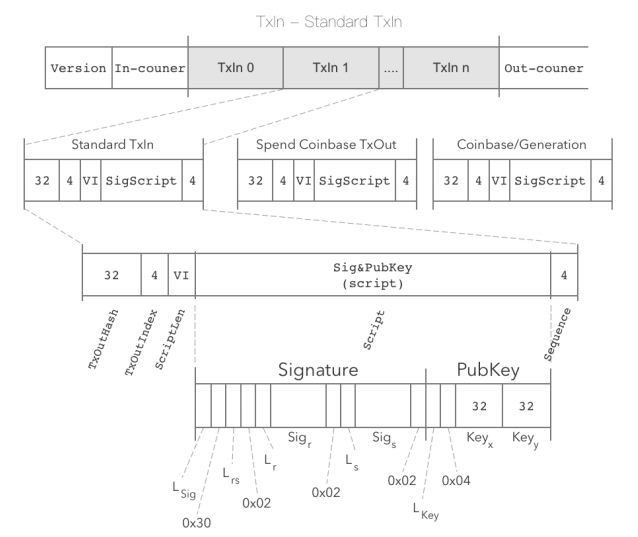
|  |  |  |
| --- | --- | --- |
| 字段 | 描述 | 大小 |
| 版本（Version） | 该交易参考的规则 | 4字节 |
| 输入数量（In-counter） | 交易输入（TxIn）列表的数量 | 1-9字节 |
| 输入列表（list of inputs） | 一个或多个交易输入 | 不定 |
| 输出数量（Out-counter） | 交易输出（TxOut）列表的数量 | 1-9字节 |
| 输出列表（output of inputs） | 一个或多个交易输入 | 不定 |
| 锁定时间（Lock time） | 锁定时间 | 4字节 |

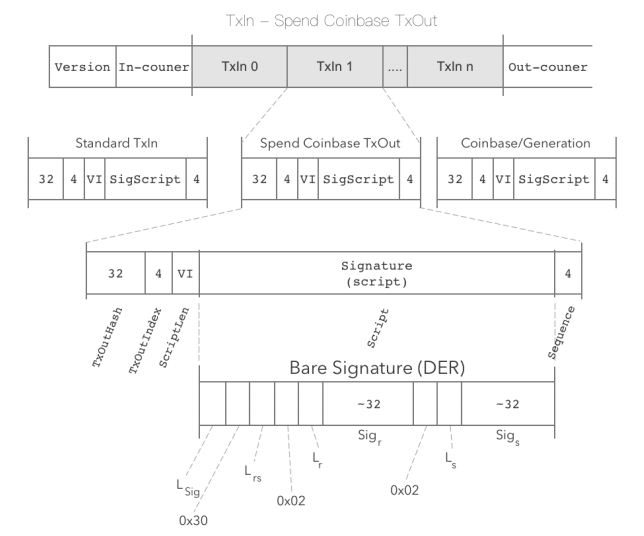
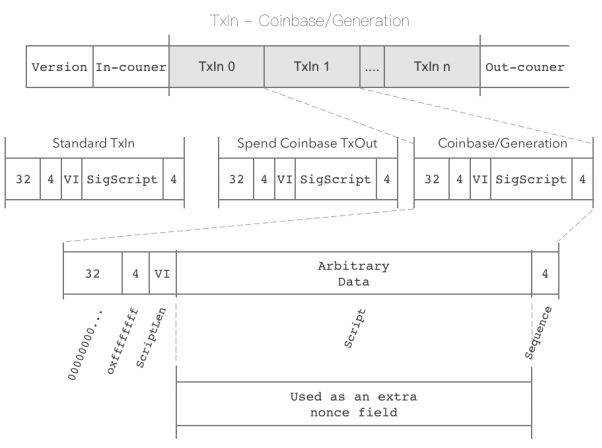
一笔交易的数据结构图如下所示：



* + 1. **交易输入**

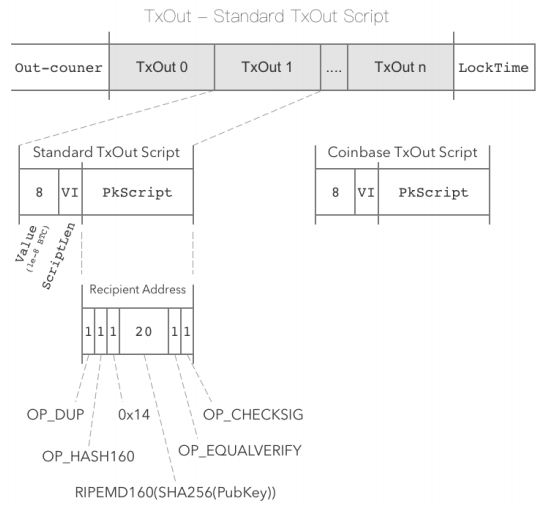
比特币的交易输入（TxIn）有三种，分别是Standard TxIn（标准输入）、Spend Coinbase TxOut（花费挖矿奖励）、Coinbase/Generation（产生挖矿奖励），对于每一笔交易输入而言**，都会有一笔由上一个持有者的私钥所添加的数字签名（也称“见证”），**用于标识持有者“消费”这笔比特币。下图分别描述了这三种TxIn的结构：

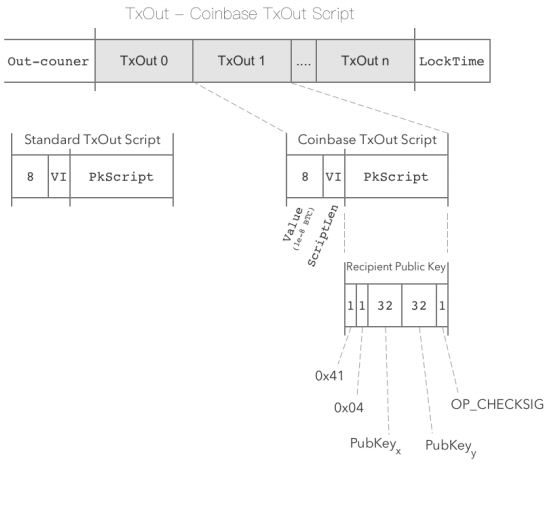


 ****

* + 1. **交易输出**

比特币的交易输出（TxOut Script）有两种，分别是Standard TxOut （标准交易输出）、Coinbase TxOut （挖矿奖励输出），下图分别描述了这两种TxOut的结构：

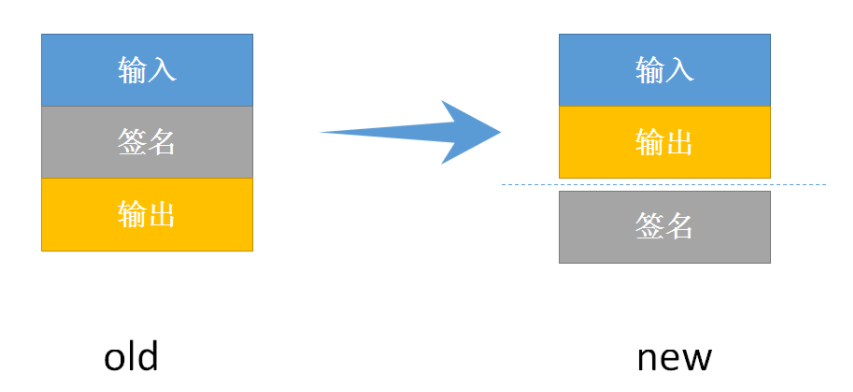




* 1. **隔离见证：**

比特币在进行转账的时候，发送方会对本次交易的信息及接受者的公钥用发送方的私钥进行一个签名，用来表示接收方“花费”这笔交易。下图表示在一个交易输入代码段里面私钥（红色代码处）的示例，从下图可以明显看到私钥还是占了很大一部字节数的：

“隔离见证”，顾名思义，就是将这个“见证”隔离开来。从一个区块里面释放更多的空间，从而增加一个区块里面交易的笔数。隔离见证后，签名信息从交易的输入数据结构里剥离开来了，形成两个数据，并在交易记录里内置一个指向签名信息的指针，让矿工进行验证。隔离见证前后交易的数据结构大致如下：



# **对交易所的风险**

在比特币分叉过程中，交易所所承受的风险主要在于分叉前后所可能带来的重放攻击。

* 1. **重放攻击**

重放攻击，这里的“攻击”不是别人对你发起的某种侵略或偷盗行为。而是因为有些区块链（有的链会做重新攻击保护）分裂后的两个分支链，都有相同的地址、私钥和交易格式。你在分裂点前的币，自动会被分裂后的两条链都承认。

如果你使用分裂点前的币发起一笔交易，在两条链上这笔交易都会有效。这就是显得你发了两笔交易，这里的另外一笔，就是“重放”。

16年的时候以太坊硬分叉为eth和etc，云币在以太坊硬分叉之后遭遇重放攻击，丢失了40000个ETC，大约价值50万人民币。

# **BTC分叉交易所应对方案**

**调研交易所：云币、火币、OKCoin、比特时代、Bittrex**

1. 分叉时间点前暂停BTC的冲提功能。（为了防止充值回滚和提币时的重放攻击）

2. 对分叉前的用户BTC余额进行快照，用于分叉后BCC的用户确权和分配。

3. 分叉情况讨论：

3.1 分叉失败，持有BTC的用户将只拥有BTC一种余额。

3.2 分叉成功，为持有BTC的用户分配等额的BCC。

4. BTC网络稳定后开启冲提功能。

5. BCC网络稳定后开放BCC提币功能。

# **为应对分叉对交易所的建议**

1. 分叉币种冲提功能后台可配置。
2. 灵活的用户余额快照机制。
3. 如若BTC分叉越来越多，可以将代领分叉币作为产品亮点进行产品设计和宣传的侧重点。