2018-05-21 陈浩



```
第25讲 | 比特币专题(二):扩容之争、IFO与链上治理
朗读人: 黄洲君 09'56" | 4.56M
```

今天,我就来讲讲比特币扩容之争的来龙去脉,并且透过比特币的扩容之争,我们可以聊一聊其背后的区

块链链上治理问题。

社区治理的难题:如何让社区达成一致。 扩容的需求是由于比特币的使用人数逐渐增长,于是比特币的网络也日益拥堵。关于如何解决这种网络拥

方案一:极端扩容,直接将区块的上限进行扩容,它的优点是可以快速解决问题,缺点是十分直接,

- 方案二:隔离见证,要求坚守 1MB 的容量上限,通过隔离见证的方法绕过 1MB 的限制。这种方式改 动比特币交易的结构,它的优点是结构的改变可以带来崭新的特性,缺点也不少,不但花费的时间较
- 长,用户的使用感知也并不算完美。 社区就上述的两种方案产生了不同的分歧(分叉),从而产生了极端扩容派和隔离见证两个派别,派别之 间谁也不服谁,对峙十分激烈。

第三个派别:调停和解派系。 至此,社区中形成了极端扩容派、调停和解派、隔离见证派三个派别,他们开启了漫长的拉锯战,中间

也有达成过短暂的三次共识(92 共识、香港共识、纽约共识),调停和解也一度将极端扩容的上限从 20 降到 8M, 甚至是 2M。但是,一切的努力,还是不了了之。

叉出一条没有 隔离见证的链,分叉之后的币就是比特现金(BitcoinCash),缩写 BCH,而隔离见证则 成了现在我们看见的比特币。至此,扩容斗争进入双链对抗的时代。 关于扩容之争详细的来龙去脉。如果感兴趣的话,你可以查阅相关资料,一探究竟。

扩容之争引起的 IFO 扩容之争基本在 2017 年 11 月结束,比特币硬分叉出比特币现金已经成了定局。比特币现金的出现还带

来了一件新事物,就是 IFO——Initial Fork Offering,也就是分叉比特币形成新的数字代币,这其实就是

ICO 的替代品。 这里要提一句,2017 年 9 月 4 号七部委发文明令禁止 ICO,所有和人民币挂钩的交易所都必须限期关

叉带来了全新的灵感,于是 IFO 应运而生。 怎么理解呢?我们之前讲过 ICO,这里来回顾一下,ICO 的中文名是首次代币发行,又称为区块链众筹,

这是一种新型的融资模式,投资者可以用手中的比特币 或其他代币投 到其他的区块链创始项目。 ICO 从本质上来说就是一纸白皮书,接下来全靠吹,忽悠散户投币,"我要出一个新的代币了,你们快来

快来买吧!"靠着与比特币的连带性,IFO 打了一记集资的擦边球。 所以国内诸多项目方和经验资深的投资方一拍即合,搞 IFO 吧。但是 IFO 比 ICO 限定在只能从比特币上 分叉, 所以技术的发挥仍然有限。

一时间,除了比特现金,一共出现了 9 个比特币分叉项目,发行总量都是 2100 万,区别在于附加功能, 例如区块时间调整、区块大小调整、是否有隔离见证、未来会加哪些功能等。

它们分别是下面这些项目,收录可能不全,你了解即可。 1. 比特币黄金,Bitcoin Gold,简称 BTG,区块大小 1M,有隔离见证功能,区块时间 10 分钟。

3. 比特币钻石,Bitcoin Diamond,简称 BTD,出块时间 60s,免手续费转账,比特币 10000:1 领取,

持币有 POS 利息。 4. 超级比特币,Super Bitcoin ,简称 SBTC,支持智能合约,闪电网络和零知识证明功能。

2. 比特币 2X, BitcoinX, 简称 B2X, 区块大小 2M, 有隔离见证功能, 区块时间 10 分钟。

6. BTP(比特币白金)总量 2100 万, 其他信息不详。 7. GOD(比特上帝)分叉,总量 2100 万, 不挖,直接分发给用户,项目发起人郭宏才,人称宝二

5. LBTC(闪电比特币,基于 DPoS 共识,需要重新开发,点付张银海为中国区负责人。

- 爷。 8. BUM(比特币铀)分叉,总量 2100 万,其他信息不详。
- 9. Bitcoin Silver (比特币白银),总量 2100 万,其他信息不详。 链上治理
- 链上治理指的是人们直接在区块链发起社区提案,并进行决策的过程。 这里首先要求的是链上支持基本治理协议,这套协议可以规定或强制执行提案,链上治理直接决定了区块

链本身的发展方向。链上治理的参与方包括了投资者、使用者、开发者、矿工四类人群。 链上治理与链下治理的区别在于,区块链本身是否提供强制执行的机制让少数服从多数。

在链上治理协议中,参与者需要 可以通过投票参与治理,而链下治理中,多数通过提案、社区见面开会

各种类型的链上治理

信息表示支持某项提案,例如矿工可以在区块中填写 NYA 表示支持纽约共识。

等多种线下线上互动方式,让整个社区达成一致,扩容之争中的三次共识就是典型的链下治理。

1. 比特币 BIP 和区块投票 虽然比特币没有提供完整的链上治理机制,但是 比特币也支持简单的投票机制,例如在区块中写入共识

但这一切都是基于比特币的 BIP,首先得有 BIP,才能发起投票。BIP 的组织架构比较社区化,主要由

Github 上的一些开发者和核心社区成员组成。

2. 以太坊 Gas limit 投票

的发展。

矿工的所有行为 也是非强制性的,当真正发生主网升级时,矿工仍可以选择不升级 ,这将带来分叉,也 是所有人都不愿看到的。

以太坊上提供了对 Gas 消耗的上限参数——Gas limit,矿工通过投票选择增加或减少 Gas limit,Gas limit 决定了单个区块上可以处理的智能合约数量, 但这仅针对这一项细分功能,并不能决定整个区块链

力。 3. 比特股 BTS 和柚子 EOS 的链上治理

我们在前面的文章介绍过 EOS 区块链链上治理结构——区块链宪法。实际上宪法也没有强制约束力,但

EOS 和比特股的治理结构来自于 DPoS 算法提供的投票过程,投票是根据币的数量作为权重的,使用

实际上,以太坊的发展受 Vatalik 本身影响比较大,核心成员和早期资本的推动是以太坊治理的主要源动

者、投资者、开发者、矿工这四种角色中,其中把矿工和投资者进行了合并,受资本的要挟,风险比较 大。 以上治理结构,我们把比特币和以太坊归为一类,这类倾向于链下治理,EOS 和比特股倾向于链上治

是它成为了一种社区强制约束力,类似宣誓过程。

无论链上治理还是链下治理方式都存在一些问题。

理。 链上治理的几个问题

• 惰性投票,只有很少一部分人会真正地去投票。 投票权过度集中,大户持有者往往话语权更重。 链下治理相比链上治理,更接近我们现实社会的方式。链上治理不是一个设计问题,它是社区制度问

升级的实际执行者矿工总是理性的,也就是追求自身利益最大化。

了可开发性。 例如链上治理至少存在以下几个问题。

链上投票可能也会遇到类似的问题。 2. 女巫攻击

目前区块链很难 映射现实中人的身份,如果按照身份去投,大户是可以扮演多个伪造身份进行投票的,

在产生区块链数字身份之前,链上治理只能依托于币的数量进行权重投票。这便造成一个代币一票,持币

当所有人都觉得别人会投票的时候,也就没有人投票了,这个典型案例是英国脱欧公投。区块链上进行

题,"如何让区块链更好地发展"相比"区块链项目应当设定什么样的发展目标",是排在第二位的。

社区在自身追求目标的过程中,会自发地找到最佳治理结构,人为设计可能会有诸多漏洞和缺陷,也限制

这其实是女巫攻击的延伸,链上治理节点可以承诺将获得的收益与其他节点进行分享, 这种拉票方式其 实就是贿选,如果恶意节点可以通过贿赂成为记账节点, 进而左右区块链的升级过程,后果非常可怕。 目前创始团队进行控制式治理是最常见的,在社区强大后,创始团队再退出,让社区自己运作,是比较典

3. 贿选

总结

多的选民有更大的话语权。

【扩容之争】参考链接:

1. 公地悲剧

型的"中本聪模式"。 链上治理其实是一个很热门的话题,它关注的是区块链自身的发展,很可能会是区块链的一个重要研究方 法, 但是这并不是技术所能解决的, 所以并不太乐观。

今天带你了解了什么比特币的扩容之争,又从扩容之争谈到了区块链治理,区块链治理没有明确的最优方

好了,本期的问题是,区块链最终会发展出有效的链上治理结构,来保证所有人的权益吗?你可以给我留

案,本篇更多地是带你了解了区块链行业的现状,希望能带给你一些新的思考。

言,我们一起讨论。感谢你的收听,我们下期再见。

https://zhuanlan.zhihu.com/p/30930715

版权归极客邦科技所有, 未经许可不得转载

你的区块链入门**第一课**

精选留言 wind53880 既然区块链有链上治理和链下治理之说,那现有区块链项目/公司通常设置怎样的治理结构呢?通常组 织架构又怎样呢? 👙 2018-05-22 作者回复 除了比特币其他都是中心化运营,通常的模式有基金会和实际执行的公司主体。 2018-05-29 **6**0 请教陈老师一个问题:现在比特币和比特现金虽然有8倍差距,但现在有一种观点认为这个差距会缩 小,甚至有可能反超,你觉得呢? 2018-05-29 "区块链最终会发展出有效的链上治理结构,来保证所有人的权益吗?"这个问题关取决于区块链项目 本身的激励机制,如果激励机制合理,即使在项目发展初期出现了权益不均的情况,最终会随着项目发

从只有少数活跃投票而看,这也就说明区块链技术现在面临的最大问题是:互联网的群发性。石润婷教 授提出的鲁棒性。休眠者多于活跃人数,从而影响投票权威。 2018-05-26 作者回复 是的,投票惰性和公地悲剧。感谢分享。

0 0

60

60

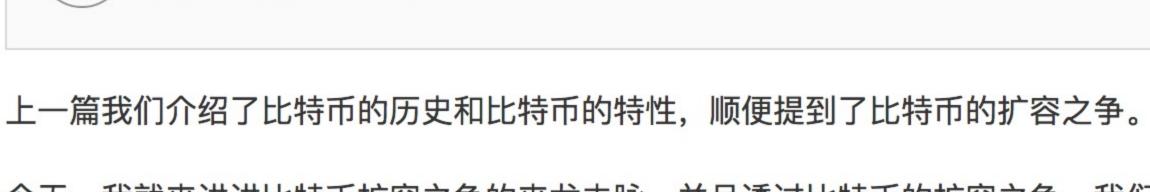
2018-05-24

作者回复 你好,可以的语句有些歧义。

实际指,开发实现隔离见证的时间相比直接扩容的时间要长,风险要高。而不是指交易验证

个人感觉专题内容真的很散哈,能在开篇之前,按照结论先行,直接读完该篇后,学到什么或者了解到 什么东西? 文章不是咬文嚼字越专业化,就越好,反而越接地气越容易理解

谢谢你的建议。其实有点众口难调啊,有人反馈我的分享太浅,需要再深入。 事实上区块链很多内容还没有定论,我后续文章尽量按照你的建议调整一下哈。 2018-05-24 zjhiphop **6**0 有了数字身份之后,可以确保所有用户投票,消灭重复投票。但是贿选投票可能还是会存在,如果贿选



扩容之争

扩容之争是比特币历史上影响较大的事件, 它也是比特币社区治理的经典案例。扩容之争的背后其实是

堵的问题,比特币社区出现了两种不同的解决方案。 只能舒缓一时的拥堵,并没有从根本上解决问题,更不能带来新的特性。

于是又出现了一些人开始试图调停双方的矛盾,希望社区不要分歧,可以达成一致。这一类人群就构成了

社区分歧仍然逐渐加大,最后比特币产生了硬分叉。一条链变成了两条。极端扩容派在比特币主链上硬分

闭。 "一刀切"政策让 ICO 在国内基本死掉了,于是国内的人坐不住了,就纷纷开始寻觅替代品。比特币的分

买吧。" 而 IFO 的集资依靠的是与比特币的关联,"我要出一个代币了,这个代币是由比特币分叉出来的哦,你们

展而解决。 2018-05-29 徐蓒会 金鸟科技

> 2018-05-29 区块链有点乌托邦

隔离见证花费的时间较长是从何说起 2018-05-23 2018-05-29

随笔川迹 2018-05-21 作者回复

可以解决,那么人人平等的投票会实现 2018-05-21