证明之证明:

一种继承工作量证明安全性，兼具去中心，免信任，透明和可扩展性的的方法

VeriBlock, Inc.

Maxwell Sanchez
Justin Fisher

Version 1.0n 1.0 版本

摘要

证明之证明共识协议能使区块链从其他区块链继承工作量证明级别的安全性，打造拥有比特币安全级别的生态。这种生态将证明之证明作为区块链安全机制间接实现了比特币分流可扩展性。受益于分级安全模式，使所有区块链在比特币级别环境下运行，进而推进其他可扩展性尝试，如链下转账网络和侧链。我们设想的是继承比特币 PoW 工作量证明但无需比特币矿工介入和授权的方法，无需中心化机构和协作节点，无需对接受此协议的区块链强加任何技术限定。

1. 介绍

当下区块链领域面临的最大问题之一是区块链能够获得和保持的共识，随之而来是对新科技的安全性各种争论。

对于 pow 工作量证明遇到两大批评：1. 能源浪费 2. 如果算力降低，区块链安全性变弱。对于电力消耗的批评并不见得站得住脚—电灯泡的灯丝也能称之为低效导体，尽管他能发光。诚然，相较于同算法的大型虚拟货币，使用 PoW 工作量证明的小规模虚拟货币更容易成为低成本攻击的受害者。
对于上述批评，人们提出并开发了多种不同的共识机制，包括 pos 权益证明（该机制中用户持有原生代币进行挖矿）；PBFT 实用拜占庭故障容错算法；瑞波协议共识机制等。

（演进了传统 RAFT 和 Paxos 等经典共识机制后的思想，在大规模非信任系统，协作节点或者可信节点上运行，这些节点在网络中解决共识冲突）

上述这些共识机制采用了权衡折衷手段，减少 PoW 工作量证明共识机制所拥有的优点：坚实的安全性，矿工参与的非信任非许可性，节点间网络历史数学验证式传递，以及高昂的攻击成本等。

我们的证明之证明共识协议解决了上述顾虑，利用一个现存强大的 PoW 区块链的算力去保障其他区块链的安全性。

2. 以前的技术

以前存在过利用现存高安全性区块链的尝试。2011 年，多个区块链，比如 Namecoin，采用了合并挖矿和 AuxPoW 协议，使比特币矿工同时挖比特币和其他链。2013 年，Mastercoin（现 Omini）发布了通过在比特币区块链嵌入数据，寄生在比特币之上的协议。

2.1. 合并挖矿 （AuxPoW）

合并挖矿让一个主区块链的矿工同时在一个或多个辅区块链上挖矿。主区块链本身不需要修改，允许其他区块链使用 AuxPoW 进行合并挖矿。为了合并挖矿，矿工必须首先为辅区块链构建有效的块，然后在他们试图挖的主区块链中包含这些块的一些证明（通常通过在主区块的交易记录中嵌入辅区块链的哈希）。如果矿工成功地解决了满足一个或多个合并挖矿或主区块链的目标下的工作量证明，则将相应的块和工作量证明解决方案组合并且中继到它们各自的区块链中。

合并挖矿需要主区块链矿工的积极参与，辅区块链继承的哈希率的百分比即是主区块链为该辅区块链合并挖矿的哈希功率的百分比。

合并挖矿不能确保大量的辅区块链的有效扩展，因为这将需要主区块链矿工跟踪和组合大量辅区块链的块。它还强制辅区块链使用与主区块链相同的哈希算法。最后，在大多数实现中，主区块链矿工攻击辅区块链的机会成本只是不合并挖矿的成本，因为矿工可以在攻击另一个辅区块链时候继续挖主区块链的矿（合并挖矿其他区块链）。

2.2. 分层技术

区块链或伪区块链通过将其全部或几乎全部的区块链写入另一个区块链来继承高度安全的区块链的安全性。这些技术的“加强”或“自觉”的客户端作为主区块链网络上的节点，寻找对其区块链有特殊意义的嵌入式数据。这些数据在它们自己的规则下被解释，以执行辅助或嵌入式区块链的操作。 以下是分层技术的一些实现：Omni / Omnilayer（以前的 Mastercoin），Colored Coins, 和 Counterparty。

主区块链中的重组导致辅助/嵌入式块链的重组。 通常，无论何时创建辅助/嵌入式块链上的事务，都会同时创建主区链上的事务。这种事务数据或其表现（散列）使用包括 OP_RETURN 和 没有公钥／私钥的“不可能”地址嵌入到主区块链的事务中。

在主区块链中嵌入辅区块链对辅区块链造成重大限制，包括块时间限制和最小存储容量。为了效率起见，这通常需要辅区块链来利用主区块链的地址格式（和相应的签名算法）。 辅区块链的用户还必须拥有并使用主区块链上的代币来在辅区块链上进行交易。最后，这些技术在主区块链上访问量大时候存在很大的扩展性问题（以事务的数量来算，而不一定是事务的大小来算）。 虽然像 Omni 等技术在点对点网络上存储和传输事务“附件”，但 Omni 区块链中的每个事务都需要在比特币上生成事务并进行广播 。

2.3. ChainDB

ChainDB 在提案中提到，在比特币中保护一个链安全需要 ChainDB 块建立节点时候协同建立一个比特币事务，它表示下一个 ChainDB 块，将安全链的最小块时间限制在比特币的区块时间内，要求完全验证的 ChainDB 节点也是完全验证比特币节点（尽管使用类似于 SPV 的嵌入在 ChainDB 链中的比特币知识的模型似乎也起作用），并提出了一个攻击媒介，比特币矿工得到 ChainDB 合法投标人支付的费用，但仍然通过包含一个备用的 ChainDB 块来定义庞大费用的交易来控制 ChainDB 区块链。此外，想修改 ChainDB 区块链的攻击者只需要支付比 ChainDB 块的酬劳高出几倍的费用，就可以在 ChainDB 块链上有一个多块重写的机会;如果每个块传输的值远多于每个块的上限，那么一个 ChainDB 区块链将具有潜在的安全性问题。

2.4. 现有技术的总结

现有的技术在辅区块链中重用一个主区块链的工作量证明在安全性级别上，局限性上和可扩展性上存在缺点。

3. 目标

证明之证明旨在实现：安全继承区块链（SI)（可以类比做参加合并挖矿的区块链或者二级寄生区块链）去继承另一个提供安全保障的区块链（SP)所拥有的全套 PoW 安全性(可以类比做父级区块链）

这种继承并不对安全继承区块链（SI)强加任何无必要的限定，无需安全保障区块链的许可，或者安全保障区块链矿工的介入，无需任何中心化网络（包括协作节点），在安全保障区块链失控时不会让安全继承区块链无法运行。同时，安全继承区块链的非挖矿用户，无需与安全保障区块链网络进行交互，也无需持有安全保障区块链的原生代币。

4. PoP 协议（证明之证明）

PoP 协议引进了一种新型的矿工，他们周期性的将一个区块链的状态发布给另一个区块链，这种公布行为可以看作为一种区块链的重组架构。PoP 的前提是某个链具有创建区块的功能，比如算力较低的 PoW，PoS 等等。

4.1. 定义

Consensus Inheriting (CI) Blockchain 共识继承（CI)链: 通过 PoP 获取安全保障的区块链，该链从其他区块继承 PoW

Consensus Providing (CP) Blockchain 共识提供（CP)链: 一种安全系数高的大区块链，安全继承区块链从其继承 PoW

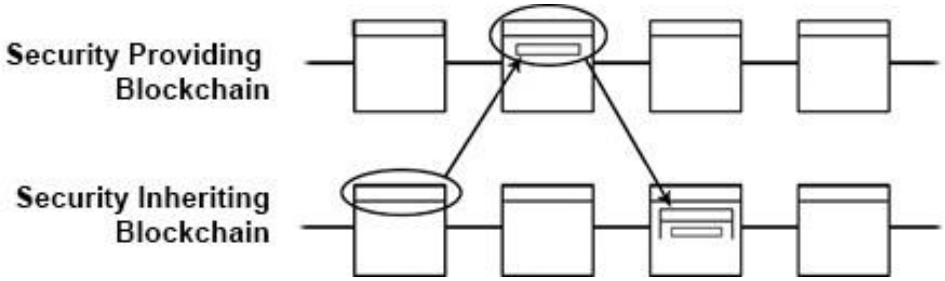
Blockchain State Data 区块链状态数据: 关于区块链实时状态的数据，比如最新块头部，区块哈希，交易转账 Merkle Root 根节点哈希值等。

***PoP Miner* PoP 矿工:** 一种新型矿工，其完成将 SI 继承区块链的区块状态数据广播到安全保障区块链的工作。

4.2. PoP 挖矿过程概览

PoP 矿工是继承区块链和安全保障区块链之间通信和交易转账的桥梁。PoP 矿工可以随时将继承区块链的实时状态数据发布到安全保障区块链上，同时兼具一些识别 ID 用来获取补偿。

有多个方法将区块状态数据嵌入安全保障区块：OP-RETURN，假地址，多重签名假地址等。PoP 矿工等待交易写入安全保障区块，构建发布证明，添加足够的确认信息以便于发布成功确认收入记账，然后再将该确认证明以特殊的 PoP 挖矿交易转账方式传回安全继承区块链。



4.3. PoP 数据发布

为了有效利用 OP_RETURN 的优点，安全继承区块链的状态数据以及便于矿工获取回报的证明信息需要限定在 80 字节之内。建议发布安全继承区块链的整个区块头部以避免我们在随后要谈到的一项安全弱点。192 位哈希值用于前一区块哈希和 merkle 树，标准区块头部仅占有 64 字节空间，其中包含版本信息，前一区块哈希的标准区块头部，前一区块哈希，merkle 数哈希值，时间戳，nbits 属性目标对象，和 nonce 随机数。 剩下 16 字节用作 PoP 矿工身份信息（如矿工地址的前 16 位）。当 PoP 矿工将 PoP 挖矿交易转账提交到安全继承区块链时，他们将包含和矿工身份认证信息前十六字节与安全继承区块链地址前 16 位相匹配的所有地址。

4.4. PoP 挖矿转账

特殊的PoP挖矿转账交易实现了安全继承区块链状态数据包含于安全保障区块链之中。比如，转账交易需要包含安全继承区块链生成的状态数据（同时包含矿工 ID 信息），包含继承区块链状态信息的安全保障区块链转账，Merkle 路径（如果集成区块链不采用 merkle 数结构，则可能是其他加密证明方式），和安全保障区块对应的区块头部。另外挖矿转账交易需要提供全部矿工 ID 信息。最后，可能会需要其他限定信息，比如足够的安全保障区块链哈希值，足以使继承区块链可以生成和验证到 PoP 矿工公布之区块链。

最简单的算法要求 PoP 矿工提交足够多的安全保障区块链头部用于生成 PoP 区块，从已知区块和高度最高的安全保障区块到包含有 PoP 发布生成的区块。

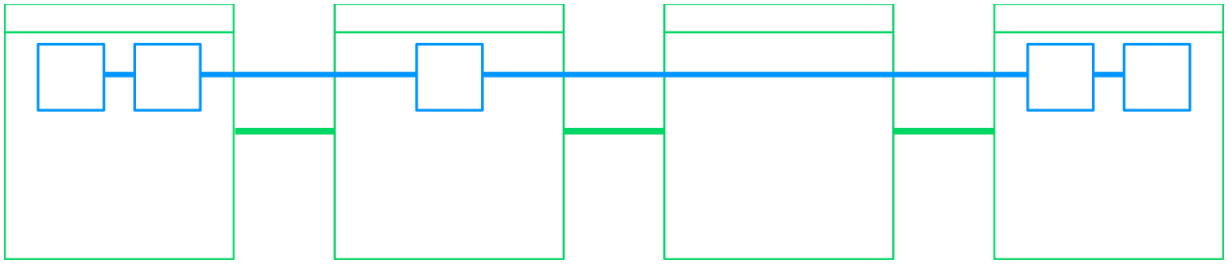
4.5. PoP 挖矿转账验证

安全继承区块链节点通过检查其状态数据，是否包含于安全保障区块来验证 PoP 挖矿转账交易，确定安全保障区块转账交易包含于该区块 merkle 数的区块头部，并且确定该安全保障区块的区块头部形成了整个区块的最长链。

检查验证安全继承区块状态数据只需要回顾发布状态数据区块。检查其是否包含于生成转账的安全保障区块链中，检查 OP_RETURN 后的数据，或者检查区块状态数据是否编入在多重签名中。接着安全保障区块转账进行哈希运算，merkle 路径生成，merkle 根嵌入到对应安全保障区块头部。因为纯 PoW 区块链的头部就足以确定区块共识，所以安全继承区块节点有足够信息保证 PoP 发布可以在有效安全保障区块中形成。

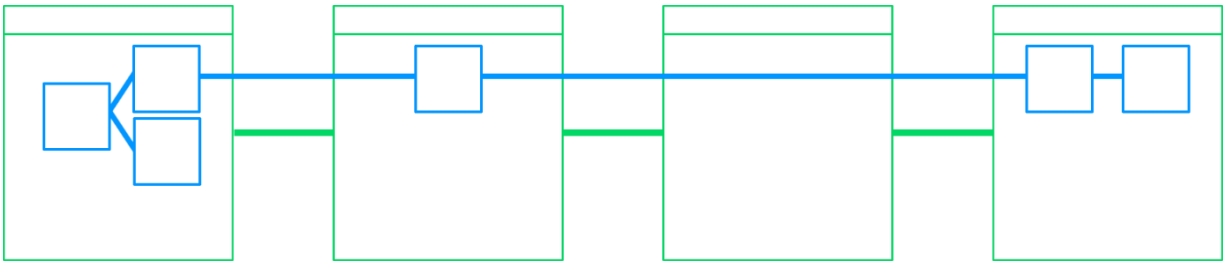
4.6. 区块格式

为了 PoP 挖矿转账交易用于共识，其必须存储在继承区块链上。并且也需要安全保障区块链的头部，这样可以追溯安全保障区块链的共识，而无需节点干扰安全保障区块链。这样，落实 PoP 的区块需要一个特殊部分用于包含安全保障区块链的头部。

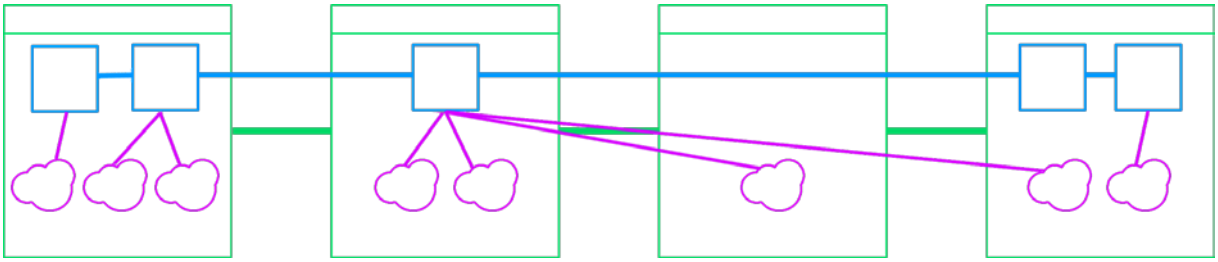


上图中，绿色代表进行 PoP 的集成区块链，蓝色代表保障区块链的头部。通过连接继承区块链上保存的保障区块头部，整个保障区块链 PoW 共识得以确认。一旦保障区块发生分叉，继承区块会包含多个竞争区块，并且允许保障区块头部嵌入到未来继承区块中，

最终解决共识冲突：



共识之共识的挖矿转账交易可理解为安全保障区块，其中发布了继承区块状态信息，存储当前安全保障区块头部（PoP 挖矿转账交易为下图粉红部分）



为实现这种转账，矿工（PoW/PoS/其他）获取 PoP 转账交易的头部数据，将安全保障区块头部嵌入。

5. 解决分叉

通过综合打分在可选分叉中选出最佳分叉。在 PoP 中，一个分叉的评定基于另一个分叉；PoP 在安全保障区块链上发布的时间顺序决定其权重，特定高度继承区块的 PoP 发布时间顺序取决于相关分叉的继承区块的第一次发布。

5.1. 安全保障区块链追踪

为了继承区块链节点解决分叉问题，节点必须评估继承区块提供的安全保障区块头部（包括各个已知分叉）。为达到这个目的，节点收集继承区块上的安全保障区块头部，通过安全保障区块链规则确定共识（找到权重最大或者算力最大的链）

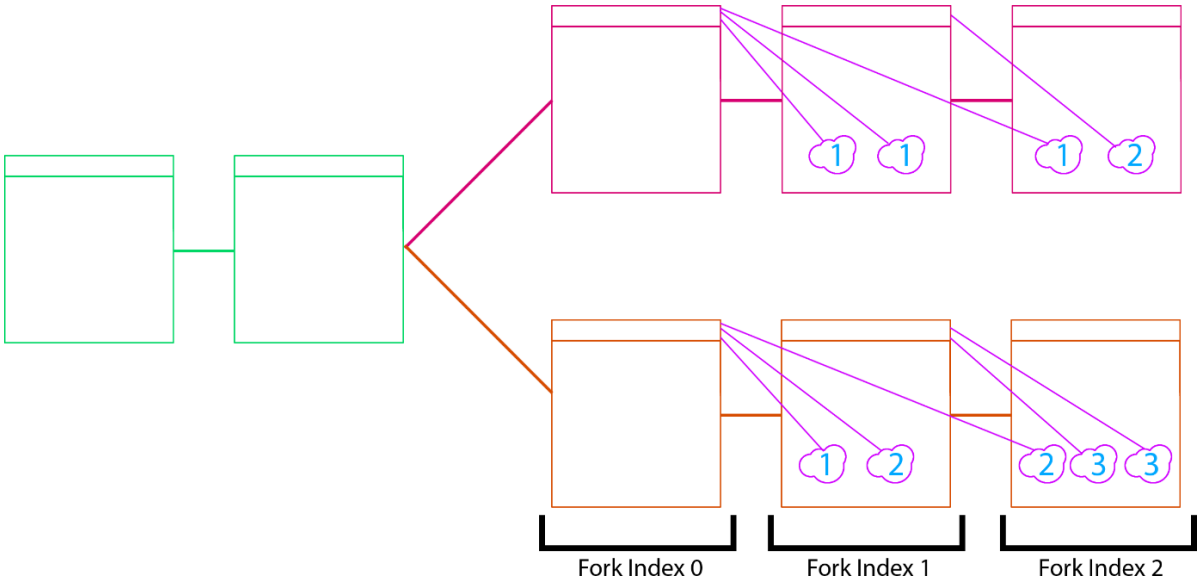
通过在重建安全保障区块链时利用所有潜在的分叉可用信息，节点可以确保，它们在安全保障区块链得到的最终画面代表安全保障区块链在任何分叉任何区块中的最新状态，允许评测犹如节点直接访问整个安全保障区块链。

通过这种机制，任何两个特定链的相对权重可以让加入网络中的节点按需计算。

5.2. 分叉权重计算

两个竞争的分叉的权重通过对两个链分叉的所有块的所有分数进行求和来计算。多个分叉的竞争块的分数通过以下算法计算：

- 对于高度为 n 的所有竞争块，在每个链中找到与高度为 n 的链的块相匹配的所有 PoP 挖矿纪录
    - 对于所有竞争链上支持高度为 n 的任何块的所有 PoP 挖矿纪录，在安全保障区块链中找到具有最早版本（以块高度算）的那个。 将此高度保存为 m
    - 对于每个竞争块 n:
        - 对于每个支持区块 n 的 PoP 挖矿纪录:
            - 如果 PoP 挖矿纪录发布到已知的最长的安全保障区块链中的块：
                - 确定安全保障区块链发布高度与 m 的差值，将 (1/((差值 + 1) * (差值 + 1)))加到当前块 n 的分数中



在上图中，安全继承区块链遇到一个分叉，有两个竞争链（红色和橙色）。PoP 挖矿记录中的蓝色数字表示他们用来发布数据的安全保障区块链的索引。因为复杂性而未显示的是嵌入在两个分叉中的安全保障区块链的块，这允许重构安全保障区块链和随后

的 PoP 事务顺序。

为了确定接受哪个区块链，每个索引处的每个块的得分会参考相同索引处的其他块来计算，并且将每个链上的所有块的分数加在一起: 竞争块第一个 PoP 的发布在分叉的 index0 处，也在安全保障区块链 index1 处。分叉 index 0, R_0 上的红色区块，得到了三个在安全保障区块链 index1 上的发布者的认同，所以它的分数是 3*(1/((1-1+1)*(1-1+1))) = 300; **R_0 = 300**. 分叉 index 0, O_0 的橙色区块， 得到两个在安全保障区块链 index 1 上的发布者的认同, 和一个在安全保障区块链 index 2 上的发布者的认同, 所以它的分数是 2*(1/((1-1+1)*(1-1+1))) + 1*(1/((2-1+1)*(2-1+1))) = 225; **O_0= 225**. 类似, **R_1 =** 1*(1/((2-2+1)*(2-2+1))) **= 100 以及 O_1 =** 2*(1/((3-2+1)*(3-2+1))) **= 50**. 任何一个链中的最后一个块不会有权重证明，因为在它后面没有区块为它背书。; **R_2 = 0 以及 O_2 = 0**. 总结来说，红色链的权重为 300 + 100 = 400，橙色链的权重为 225 + 50 = 275.因为 400> 275，所以红色链是更受认可的区块链。

尽管橙色链包含 5 个 PoP 挖矿记录，而红色链包含 4 个 PoP 挖矿记录，红色链交易记录的相对及时性导致其具有较高的权重证明，使其成为更好的链。

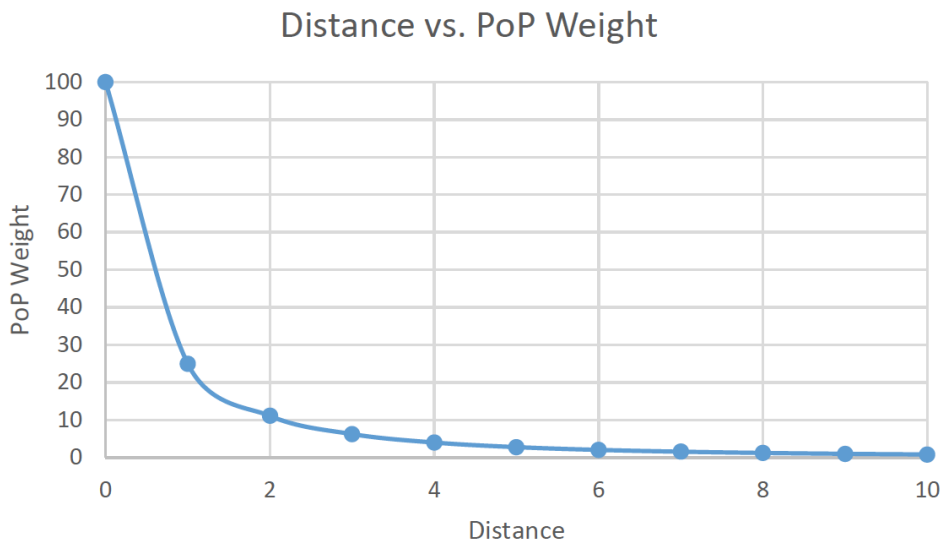
5.3. 分叉方案设计解析

基于安全保障区块链的 PoP 挖矿相对权重的使用，让攻击者非常难在脱离安全保障区块链的任何时候凭空生成一个分叉。

因此，攻击者需要依靠合法网络生成潜在的分叉，并且必须通过在安全保障区块链中发布共识继承分叉的块哈希来完全公开的进行。任何人都可以监视安全保障区块链正在建立的分叉和延迟接受事务直到分叉解决了。并且安全继承块链网络可以使用诸如基于平衡的投票之类的机制来实现附加功能来使这些攻击者的链在发布释放前无效。

5.4. 权重功能

PoP 挖矿建议的权重函数是 floor(1/((distance+1)^2)), 其中 distance 是前面描述的在 PoP 挖矿记录相关的安全保障区块和任意竞争链上相同索引的第一个安全保障区块之间的距离。可以调整该公式以更好地适应特定安全保障区块链网络的所需安全性。使用趋向 0 的功能将更快导致现有的区块链接更易于攻击，同时也增加了短期逐步攻击的可能性，攻击者在网络上产生相应的合法安全继承链块之前，试图将其共识继承链的单个块放到安全继承链块中。当我们运行更多的不同攻击场景的模拟时，这个建议的功能将继续进行调整。 下图说明了建议的 distance-vs-PoP 权重函数。



代替每次计算函数，可以使用简单的查找表:

Distance	Weight
0	100
1	25
2	11
3	6
4	4
5	2
6	2
7	1
8	1
9	1
>=10	0

在相关安全继承区块链的块索引的首次发布之后，对应于安全保障区块链块 10 个或更多个块的任何 PoP 挖掘事务没有权重。

如下面提到的潜在漏洞的解决方案，也可以应用类似的加权方案来优先考虑靠近分叉点的块的相对分数，以确保安全继承区块链需要尽早向安全保障区块链通告。

6. 潜在攻击方向和解决措施

与所有共识机制一样，对抗方可以企图强制让网络重新建立共识。在正确实现的 PoP 网络中，这些攻击的方向包括分叉安全保障区块链，构建并证明一个替代的安全继承区块链。PoP 的一些设计决策消除了简单理论上 PoP 类实现的其他潜在攻击方向。

6.1. 共识提供区块链分叉

在攻击方成功地将安全保障区块链分叉的情况下，他们可以用新的 PoP 数据重新写入分叉的安全保障区块链块中，使得它们能够产生具有较高 PoP 权重的安全继承区块链。它们能够重写的安全继承区块链的数量/长度（以实际时间而不是块来测量）大约等于它们成功分叉安全保障区块链的距离。

请注意，没有特别意图分叉安全继承块链的安全保障块链，将不会导致安全继承块链的分叉。然而，这种安全保障区块链的重组将导致安全继承区块链的 PoP 挖矿记录不再出现在安全保障区块链中，因此没有权重。进一步研究的一个领域是，如果攻击者仍然在其新的块中包含 PoP 发布者以获得交易费用，PoP 矿工可以使用某种处理来重新证明其旧证明在新的安全保障块链上的存在。

如果安全保障区块链分叉而不攻击安全继承区块链，并且安全继承区块链的 PoP 挖矿受到影响并且不再含有权重，安全继承区块链的当前安全性将下降到其自身的中间的（PoW / PoS 等）共识机制，直到 PoP 矿工将新的块状态数据发布到安全保障区块链上，并将 PoP 挖矿记录提交给安全继承块链。

6.2. 建立一个替代的高证明权重安全继承区块链

执行此攻击要求攻击方建立一个替代的安全继承区块链，其具有比当前最佳的安全继承区块链更高的证明权重。为了成功执行这个攻击（由于证明被及时评估），攻击者需要与当前的安全继承区块链同时（或更快）地构建攻击块。这就要求攻击者须迅速将攻击链的块状态数据发布到安全保障区块链上，让网络用户可以看到等待中的攻击及其属性。因此，任何人查看安全保障区块链都会看到有什么块有分叉的风险，与攻击方的链相比，目前的链有多强（或弱），并且可能会使用某种手段 （例如基于投票）在攻击链发布到网络之前使其无效。

在另一个可能的（虽然更困难）的实施中，攻击者会建立一个替代的安全继承区块链，其较早的块与当前链相比具有小到几乎没有的证明权重，但是后来的块被广泛地发布到安全保障区块链中。 由于安全保障区块链上的发布者的原因，这种攻击仍然是公开的，但是它不一定会显示分叉可能发生的时机，并且在攻击链的一些较早的区块在没有证明权重的情况下建造时，也不会出现在网络的用户身上。为了减轻这种攻击，区块链网络可以轻松地将块权重加大以更接近分叉点(所以计算大概类似 $100 * weight_0 + 70 * weight_1 + 55 * weight_2 ...$), 让攻击困难或者无法实现.

6.3.发布虚假安全继承区块链状态数据

在 PoP 实现的版本中，发布到安全保障区块链的安全继承区块链状态数据不足以验证数据的潜在有效性，攻击方可以通过伪造一个不存在的潜在分叉来延迟接受交易。这种攻击不需要强制的中间共识，但是只会让攻击者变成一个滋扰，因为如果攻击者不能提供标记着安全保障区块链的数据的完整块，网络将不会分支。这种攻击让攻击者发布他们实际上没有的而表面上有效的块状态数据。

在仅依赖 PoW 立即达成共识的安全继承区块链中，可以通过要求类似 PoP 目前的方式，发布整个块头来得到减轻。这样一来，由于数据不是有效的 PoW 的解，攻击者不能发布伪造的安全继承区块链数据。

在使用 PoS 的安全继承区块链中，也可以发布证明代币年龄或类似网络资产的采矿资源所有权的附加信息，或者可以通过知情的网络参与者验证，例如完整节点（包含声称花费的代币年龄的 txid 等）。

7. 与 PoS 结合

PoP 需要创建块的中间方法（或其他分散单元的共识），并在 PoP 发布者之间维护短期共识。使用 PoW 作为中间共识机制的网络实施 PoP 是直接明了的，给 PoP 自然扩展了 PoW 般的共识。在 PoS 网络上实现 PoP 需要额外的考虑，并为纯 PoS 的长期存在的问题提供解决方案。

7.1.现在 PoS 的问题

注意：存在几种 PoS 实现方案。 PoS 不是一个单一的共识算法，而是一些密切相关的共识算法的集合，它们都具有“基于结余”（或基于未动用输出）的挖矿的共同特征，其中矿工们使用他们的本地代币结余来生成块，挖矿的“资源费用”是代币的时间价值。原本 Peercoin 实现 PoS 中存在的一些问题（例如由于固定的权益调整器导致的远程攻击）已经通过较新的 PoS 实现来解决，这些解决的问题将不会在这里进行讨论。

PoS 目前面临的两个主要问题:

1. 在启动期间，无法通过数学上展示区块链接到新节点的有效性（链具有“弱主观性”）。

2. 对于“没有权益”的问题，只有一个短期的解决方案（最后的'n'块）。

这两个问题都归结为 PoS 的主题 - 数星期，数月，或数年后，在区块链历史中的任意点，代表网络代币所有权的“临界质量”的一些私钥可用于产生更有效的网络分叉，并且不要求任何代币的现有所有权。此外，不能证明没有一方可以访问大量的网络代币。 Slasher 协议提出了在短期内解决“没有权益”问题的惩罚性制度。

7.2.启动过程中有效性的数学演示

传统的 PoW 系统具有“最佳区块链”的客观定义（需要创建最多累计工作的区块链）并且假设启动节点具有对块链网络的无限制访问，则该节点将始终能够独立地确定最佳块链。

在纯 PoS 系统中，上述临界质量所有权问题的解决方案只是作为协议的一部分，可以防止任何节点返回超过一定数量的块。这种系统导致回滚检查点系统，其中每个节点简单地拒绝从当前'最佳块链'视图去除多于一定数量的块'n'。因此，如果客户端使用旧的代币所有权来创建开始于 n 个块以前的分支，网络上的节点将简单地拒绝分叉。然而，一个启动客户端可能首先提供数据给非法的区块链，并且随后拒绝在非法链上重新插回 n 个块，永久地（无需人为干预）阻止它们跟踪正确的块。

PoP 为此问题提供了一个简单的解决方案，使用 PoP 的区块链具有由 PoW 安全保障区块链中定义的可数学验证的“最佳块链”。

7.3.超过 ‘n’ 个区块 “没有权益” 的解决方案

目前解决的“没有权益”的解决方案是客户端忽略从当前区块链中移除多于 x 个块的分叉，如上所述。

因拒绝执行多于 n 块的区块链重组，而提出了一个有趣的攻击方向：在新块的传播过程中部署一个 y 个区块的分叉，并留下网络的一部分（谁还没有看到最新的块，并且想回退 x 块）永久的不同步（ 没有人为干预）从已经收到新块开始的部分，并拒绝分叉回 x + 1 块。这种攻击的合理性和潜在的损害随着块传播时间的增加而增加，这可能是由更大和更复杂的验证块引起的。 由于我们无法在其他地方找到任何这种类型的攻击，所以我们会在附录 A 中进行描述。

实现 PoP 将确保在区块链历史中在给定时间获取关键的代币所有权不能用于攻击网络，因为随同的 PoP 发布者由于不够及时而不存在或不相关，让客户端移除关于最大分叉距离的规则，因为分叉任何重要部分将需要成功并且同时攻击安全保障区块链。

事实上，成功的无竞争的 PoP 支持块作为一个有效的“最大软分叉距离”，随着 PoP 加权算法的难度越来越大，在某一特定历史点之前创建分叉的难度变得非常不可能。

8. 附录 A: 有限重组距离打断攻击

8.1. PoS 短期共识保护回顾

在短期内，纯 PoS 块链可以通过在一段时间内要求押金（或冻结资产）来避免“没有权益”的问题，以便能够对这些代币进行 PoS 采矿（一种被认为是 Ethereum 的方法，称为 Ethereme 开发者的“Slasher”）。在正常的 PoS 系统中，尝试在所有可能的分叉之上产生 PoS 块的成本可以忽略不计。当一个 PoS 矿工接收到两个或更多的竞争块时，将会尝试在这两条链上创建，或者有可能扣留无法挖掘顶部的任何竞争块。然而，通过冻结资产，网络可以通过允许“赏金猎人”来监视这种行为来惩罚那些采取这种行为的矿工，提供加密证明（例如来自同一个矿工的两个签名，投票给相同高度的竞争块），并且接收一部分冻结的代币。

最初的短期分叉攻击需要立即在攻击之前拥有网络中的大部分代币，这使得它们在很大程度上是不可能的和不经济的。

“权益粉碎”攻击也是在短期内无用的，因为由 Blackcoin 和 Neucoin 等项目实现了最低代币年龄和动态权益调整器等方案。

PoW 网络中不存在这些问题，因为在一个链上构建的计算能力不能用于在另一个链上。

8.2. 长期攻击

从长远来看，大多数保护共识的手段是无效的。 冻结的押金最终会被归还，长时间允许攻击者出售他们代币的整个仓位，或者获取很久以前持有的大部分代币的私钥，并且粉碎攻击会成为可能，因为能够可靠地重写过去块的临界质量的攻击者可以在他们算力范围之内挖掘许多潜在的块（每个具有不同的事务/事务顺序，就像权益修改器那样改变东西。如果给予足够的算力，就可以创建比当前的更有效的区块链，这样就可以获得区块链过去的临界质量的代币所有权/控制权。

试图进行这种攻击形式的攻击者目前不一定拥有任何代币，更有可能对导致服务大量中断而不是进行双重攻击感兴趣。

8.3. 当前对长期攻击的解决方案

为了消除长期攻击重写多年的区块链历史纪录的可能，PoS 网络上的客户端被简单地编程为不接受在'n'块之前的网络分叉的重组。这使得新的启动节点可能永久性地搁置在不正确的分叉上，但是在正常操作下不会导致中断任何连接中的节点，或比网络中添加 n 个块更频繁连接的节点。

选择 n 为最大重组深度取决于几个因素，包括代币被锁定的周期（如果在基于押金的 PoS 系统上，像 Slasher 的建议），预期攻击者获取旧私钥/卖出代币仓位的时间，网络

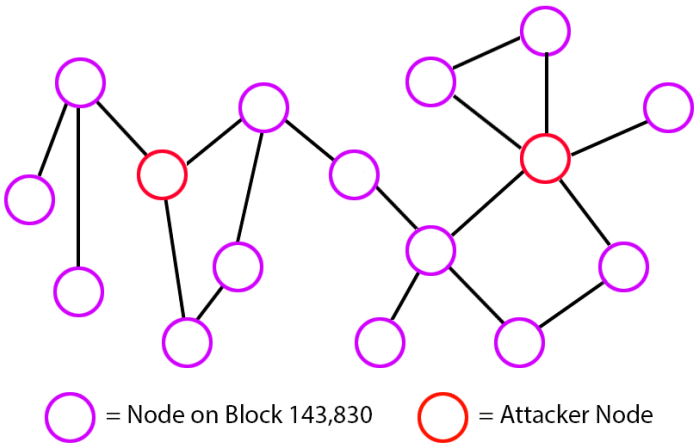
上的块的速度等。

太小的 n 使得网络容易不同步（因为即使非常困难的攻击在非常短的时间段中由于概率是可能发生的），并且太大的 n 使得长期攻击更有效。

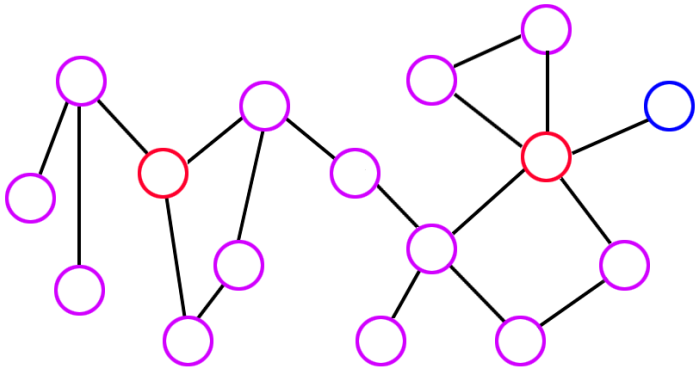
8.4. 最大重组深度的问题

如果攻击者能够在第 n 块之前创建一个分叉，而当前块仍然在网络上传播的时候，攻击者可以释放此分叉（意味着网络上的一些节点与其他节点不同）。

在像 Neucoin 这样的区块链，最大重组深度为 43,430 块，如果网络上的当前块高度为 143,830，那么释放一个回退到 100,000 块的分叉将会被所有节点接受。然而，一旦网络处于块 143,831，则释放回退 100,000 块的分叉将不会产生任何结果。

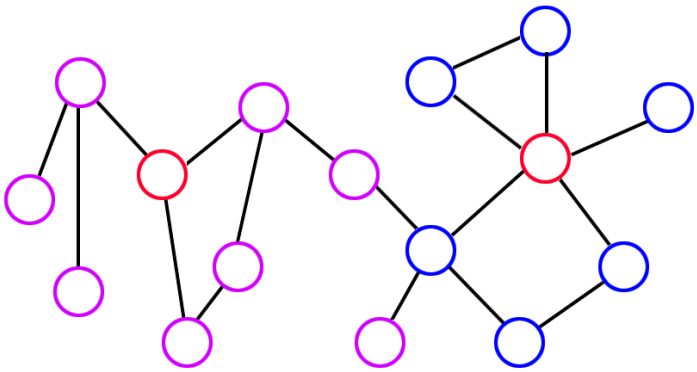


= Node on Block 143,830 = Attacker Node

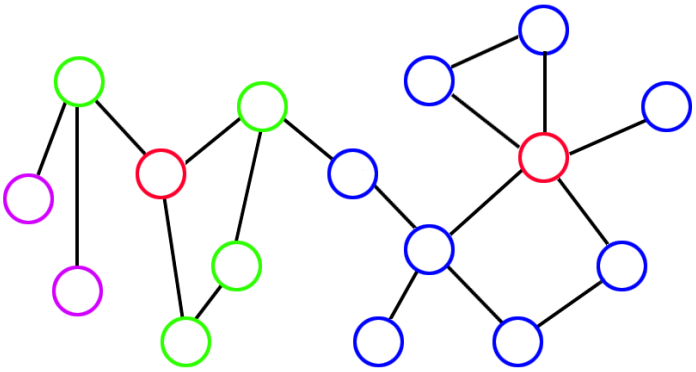


= Node on Block 143,831_a

Attacker learns of block 143,831 from one owned node

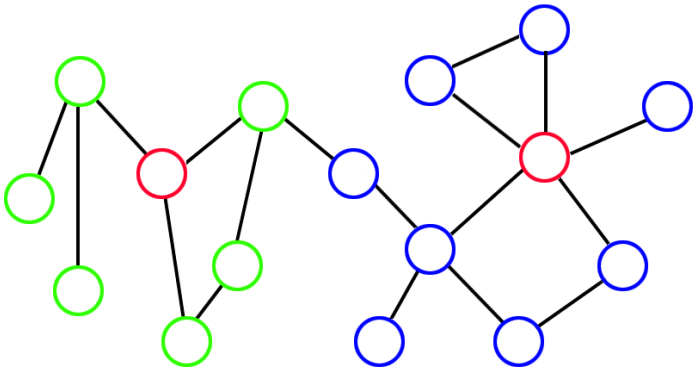


Propagation of Block 143,831_a continues



= Node on Block 143,831_b

Attacker releases fork back to 100,000 which ends with block 143,831_b



Network settles, nodes on block 143,831_a and block 143,831_b are unable to reach consensus because they diverge at block 100,000, and switching from _a to _b or from _b to _a would require a reorganization deeper than 43,830 blocks.

由于新块的网络/处理时间延迟，在整个网络中存在一段时间处于块 143,830 和块 143,831 之间。在此期间，控制着仔细分布和良好连接的节点的攻击者可以在 143,831 块刚在网络中被观察到的时候释放一个分叉。因此，只知道 143,830 块的节点将接受该分叉并覆盖了 143,830 个历史块（并且将结束在分叉的最后一个块上，即 143,831）。然而，接受合法块 143,831 的节点将不接受网络上传播的分叉。在这一点上，网络被分解成两个部份，它们都有一个表面上有效的块 143,831。分裂的双方不能调和并确定哪个块是正确的，因为任何一方接受另一方的块状物将需要重新组织 143,831 个块，根据协议，任何客户端都不会进行人为干预。

在非惩罚型 PoS 系统中，最佳自助采矿策略涉及对所有可用的区块链进行挖矿，有可能从早期的共同点产生的几个竞争分叉仍然并行构建。当这些竞争分叉的共同祖先的长度达到 n 时，客户可能会让彼此永久地不同步，因为他们单独选择这些分叉中的一个，并拒绝分叉到任何其他分叉中，因为其他分叉需要比它们愿意范围中的还要再深入的组织网络。

8.5. 减轻

这种攻击要求 n 足够大，以至于攻击者可以根据过去拥有的私钥成功构建一个“自我维持”的块，或者 n 足够小，以致产生距离为 n 的短期攻击。将 n 设置为尽可能远离两个极端值，会显著降低攻击者执行此攻击的能力。

或者，实现 PoP 消除了对最大重组深度的需求（并且使得几乎不可能实现长时间的重组），消除了这种永久不同步攻击的潜在风险。

9. 附录 B: VeriBlock 区块链

大多数块链都希望从比特币继承共识的安全性。 为了缓解由块限制和交易费用上涨引起的问题，10 分钟的区块时间，使用 OP_RETURN 发布数据的 80 字节限制，和大量的无组织的非关联数据通过比特币区块链进行排序，我们提出了一个中间聚合块链：VeriBlock。VeriBlock 旨在使用 PoP 直接与比特币获得安全性，并允许其他区块链直接将任意块状态数据发布到 VeriBlock，VeriBlock 由代理发布到比特币上。

9.1. 整合 VeriBlock

使用 VeriBlock 保护的区块链将使用它的库来自动跟踪 VeriBlock 和比特币的共识，然后慢慢改变块格式和奖励结构，以适应和奖励 PoP 矿工，并更新其网络共识的规则，以便在解析分叉时查询 VeriBlock 库。

9.2. VeriBlock 设计

VeriBlock 基于 PoW 的网络，旨在处理使用 PoP 直接处理到比特币的小型区块链上的简单事务（无脚本）。 快速块时间（如 1 分钟）可减少发布变数，事务支持发布较大的任意数据（足以在 PoS 和 dPoS 网络使用），VeriBlock PoW 矿工自动遵循几个简单的聚合规则，以提供已发布数据的摘要（根据已发布数据的前缀对 POP 事务进行排序，并将所有潜在相关信息分组）。此外，VeriBlock 旨在提供对所感兴趣的任何安全继承区块链接上的早期攻击通知的简单订阅。 这提供了一个环境给商业，交易所，支付处理器等。（VeriBlock）取关于他们感兴趣的所有区块链的安全信息，使得与第三方的安全集成变得非常简单。

9.3. VeriBlock 优点

若要直接到比特币，区块链需要将其块头改为 PoW 网络的大约 64 字节大小（而不是普通的 80），或者选择使用更昂贵和困难的发布方式（如“不存在”的地址，多个 OP_RETURN 在多个事务等）。此外，该区块链还需要自己实现比特币的完整的 SPV 级别共识，感兴趣的用户将需要收听整个比特币区块链以进行早期攻击检测。

使用 VeriBlock，它们可以保持当前的块格式，发布更大量的块状态数据（特别适用于需要发布数据来证明有关 PoS 矿工声称要消耗块的 PoS 网络），利用更快的出块时间来发布并以适当的权重，迫使攻击事件变得越来越明显，并且拥有更高层次的 PoP 挖矿去中心化，因为每个 PoP 发布者在 VeriBlock 上的成本要低于比特币。

9.4. VeriBlock 依赖

选择使用 VeriBlock 的区块链在 VeriBlock 网络发生故障的情况下不会停止运行。 现有的 PoP 共识存储在安全继承区块链本身上并且仍然可以被使用，并且在没有新的 PoP 信息的情况下，未来的共识将简单地回归到区块链的普通共识算法（PoW / PoS 等）。

此外，若区块链愿意放弃 VeriBlock 的早期攻击检测优势（或愿意将开发工作同时放在监视 VeriBlock 和比特币上以防范潜在的攻击）可以允许 PoP 矿工使用 VeriBlock 或直接向比特币发布信息，在发生 VeriBlock 问题时提供 PoP 故障转移。

References

[1] Peercoin Whitepaper [https://peercoin.net/assets/paper/peercoin-paper.pdf]

[2] BlackCoin PoS Whitepaper v2 [https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf]

[3] Neucoin Whitepaper [http://www.neucoin.org/en/whitepaper]

[4] Ethereum Blog Post on Weak Subjectivity [https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/]

[5] OmniLayer Specifications [https://github.com/OmniLayer/spec]

[6] Counterparty Specifications [http://counterparty.io/docs/protocol_specification/]

[7] Colored Coins Specifications [https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification]

[8] Merged Mining Specifications [https://en.bitcoin.it/wiki/Merged_mining_specification]

[9] ChainDB Whitepaper [https://bitpay.com/chaindb.pdf]