

# Project PAI预选混合共识机制

作者:

Mark Harvilla, PhD<sup>1</sup>

Jincheng Du<sup>2</sup>

审稿人:

Thomas Vidick, PhD<sup>3</sup>

Bhaskar Krishnamachari, PhD<sup>4</sup>

Muhammad Naveed, PhD<sup>5</sup>

## 摘要

PAI币的工作量证明 (Proof of Work (PoW)) 共识机制使用的是双SHA-256哈希协议——比特币核心 (Bitcoin Core) 使用的相同机制。这种与经典比特币式挖矿的兼容性为PAI币挖矿提供了较低的门槛, 从而使PAI币网络容易遭受所谓51%攻击等的攻击。为缓解这些风险, 本文提出了一种混合工作量证明与权益证明(PoW/PoS)的共识机制, 并为该机制如何能在成功实现的情况下解决PAI币网络固有的一些漏洞提供了详细的技术分析。本文为基于区块链的混合工作量证明与权益证明(PoW/PoS)共识机制提供了一个详细的技术概要, 包括它们在独立使用和混合模型的情形中使用时的优缺点。本文还提供了一个攻击混合动力PAI币网络的经济分析并为PAI币共识机制的未来发展提出了最终建议。

---

<sup>1</sup>ObEN公司首席工程师

<sup>2</sup>ObEN公司区块链研究者

<sup>3</sup>加州理工学院计算与数学科学教授

<sup>4</sup>南加州大学电气工程系教授

<sup>5</sup>南加州大学计算机科学助理教授

# 致谢

本报告已经过加州理工学院计算与数学科学系教授Thomas Vidick和南加州大学计算机科学系助理教授Muhammad Naveed的审核和背书。同时也纳入了南加州大学电气工程学院教授Bhaskar Krishnamachari的建议。最终还要感谢P19 Inc.总裁Ryan Straus先生为本报告作出的贡献。

## 其他贡献者

ObEN公司区块链研究者 - 方丹博士

LA区块链实验室联合创始人 - Eman Safadi女士

## 专业术语

- PoW——工作量证明 (*Proof of Work*) ; 一种共识方案, 其中挖出一个区块的概率由矿工的工作量决定。
- PoS——权益证明 (*Proof of Stake*) ; 一种共识方案, 其中挖出一个区块的概率由矿工持有的加密货币数量决定。
- ASIC——特定应用集成电路; 专门为特定用途设计的集成电路, 例如: 加密货币挖矿。特殊的设计有助于提高性能。
- DCR——Decred; 一种使用混合PoW / PoS共识方案的加密货币。
- KYC——了解你的客户 (*Know Your Customer*) ; 验证潜在客户的身份和业务意图的过程。
- Dapps——去中心化应用程序; 许多用户在具有无信任协议的去中心化网络上运行的应用程序, 旨在避免任何单点故障[2]。
- UTXO——未花费的交易输出 (*Unspent Transaction Output*) ; 一笔区块链交易中尚未花费的输出, 并可以用作新交易的输入[25]。
- P2P——点对点 (*Peer-to-peer*) ; 一个分布式的应用体系结构, 用于在对等体之间划分任务或工作量。各点在应用中享有同样的权利与义务[3]。
- DDoS——分布式拒绝服务 (*Distributed Denial-of-Service*) ; 通过许多不同来源的流量瘫痪目标机器或网络服务的攻击。

# 目录

<b>介绍</b>	<b>5</b>
<b>第1节 - 实用共识机制</b>	<b>6</b>
1.1    工作量证明 (Proof of Work (PoW) )	6
1.1.1    优点	6
1.1.2    攻击向量和漏洞	7
多数攻击	7
案例	7
条带式挖矿 (Strip Mining)	8
女巫攻击 (Sybil Attack)	8
1.2    权益证明 (Proof of Stake - PoS)	8
1.2.1    优点	8
1.2.2    攻击向量和漏洞	9
Nothing-at-Stake攻击	9
1.3    混合工作量证明与权益证明 (PoW/PoS)]	10
1.3.1    概述	10
下注机制案例	11
1.3.2    技术参数	12
1.3.3    攻击向量和漏洞	12
多数攻击	12
Nothing-at-Stake攻击	14
权益池	14
1.3.4    其他好处	15
<b>第2节 - 工作量证明 (PoW) 的哈希函数</b>	<b>15</b>
2.1    特定应用集成电路 (ASIC) 矿机可抗性	16
<b>第3节 - 建议与未来工作</b>	<b>17</b>
3.1    总体建议	17
3.2    未来工作	17
<b>附录A - 多数攻击的数学论证</b>	<b>18</b>
<b>附录B - 多数攻击的成本分析</b>	<b>19</b>
<b>附录C - 加密货币的哈希算法</b>	<b>22</b>
<b>参考文献</b>	<b>23</b>

## 介绍

PAI币 [4] 是一种基于UTXO并由PoW驱动的加密货币，相当于比特币核心的代码分支。PAI币在比特币之上引入了其他的特征和功能，例如去中心化数据共享 [5]。PAI币协议的应用包括对ObEN公司消费者个性化人工智能的认证过程 [6]。PAI币同时也是PAI生态系统的交易媒介。

作为比特币核心的代码分支，PAI币的PoW共识机制用的是双重SHA-256哈希协议。因此，PAI币与比特币式挖矿完全兼容，任何能够挖比特币的挖矿软件或设备都可以用来挖PAI币。由于存在大量与比特币兼容的哈希算力——其中大部分由于在比特币挖矿竞赛中过时而被闲置[7]——PAI币，在其当前状态下，易受潜在毁灭性攻击向量的攻击，例如51%攻击和条带式挖矿等。

Project PAI的开发人员意识到了这种情况。作为临时解决方案，PAI币目前在协议级别实行coinbase地址白名单 [8]。这意味着，当矿工提交新区块时，除了在CheckBlock()中进行的标准区块验证之外，指定的coinbase支付地址必须与挖矿地址白名单[9]中的一个匹配。这可以防止不受白名单地址控制的矿工获得区块奖励，从而阻止上述攻击向量。

Project PAI开发人员预计，Project PAI将“满足项目的当前需求”，并且“若替代方案.....在通过经验证明为实质上有益，那么这些替代方案将被采用以取代最初的基础技术。”[4] 为了满足更广泛的公共挖矿需求，Project PAI一直在努力寻找能够安全移除coinbase地址白名单的解决方案。为此，本报告提出了一项混合PoW和PoS的共识机制协议，其动机部分源于该领域当前的技术进步。采用本提议将带来一些改进，包括公共可访问的挖矿，更加去中心化，通过币下注提高能源效率，更广泛的币分配，更安全的点对点网络以及更强大的生态系统。

本报告的剩余内容安排如下：第1节概述了普遍共识机制的利弊。第1.3节详细介绍了拟议的混合共识机制。作为PoW算法主干的候选哈希函数，将在第2节中进行讨论。最后，第3节包含共识机制更改的总体建议，并概述了集成和部署的计划。

# 第1节——实用共识机制

## 1.1 工作量证明 (Proof of Work (PoW))

经典且最常见的共识机制是工作量证明 (PoW)。在PoW中，创建有效的区块需要矿工为一个“难以”计算但“易于”验证的数学问题提供解决方案，并以此作为工作量证明的演示。一般而言，给定矿工将新区块添加到区块链的概率与该矿工可用算力的多少成正比。PoW的一些常见缺点是越来越高的物理资源使用成本，以及由随时间推移而越来越集中的哈希算力所导致的越来越低的用户参与度。

### 1.1.1 优点

PoW的一些显著优点包括 [10]:

- 抗DDoS攻击
  - PoW对参与者的行为施加了某些限制，因为这项任务需要付出相当大的努力。有效的攻击通常需要巨大的计算资源，高昂的经济成本能一定程度上遏制攻击。
- 币持有量的影响很小
  - 如上所述，形成新区块仅取决于计算资源，与入注多少无关。因此，即使是大量币的持有者也无法直接获得为整个网络做出决策的权利。

## 1.1.2 攻击向量和漏洞

### 多数攻击

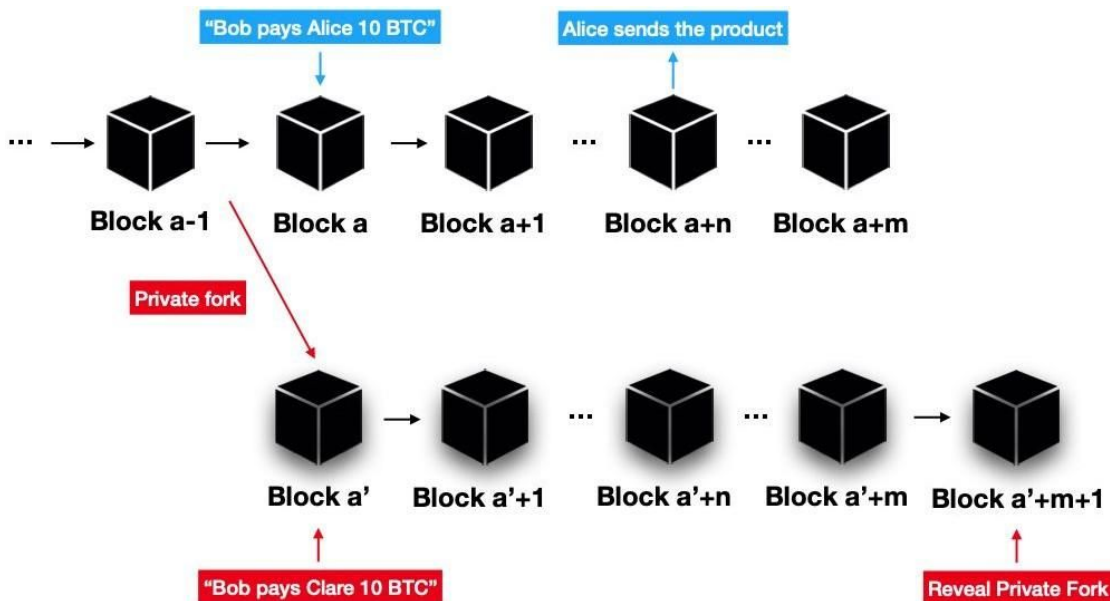


图 1. 双花攻击 (Double Spend Attack)

当某一网络参与者控制超过50%的网络哈希算力时，可能会发生多数攻击（即51%攻击）。一旦比其他所有网络参与者拥有更多的哈希算力，攻击者平均可以比网络其他参与方更快地生成和验证区块。这与最长的链规则 [24] 相结合，可以允许攻击者将非法交易注入区块中并随后验证它们。多数攻击的一个可实现的结果是双花（double spend），如下所示。

### 案例

如图1所示，攻击者Bob通过向商家Alice发起交易来从Alice处购买产品。该交易包含在区块a中，其中a是整数索引。Bob私下偷挖了另一条区块链分支，其中一个欺诈性的双花支出交易包含在区块a'中。在等待n次确认之后，即当区块a+n被挖时，商家Alice将产品发送给Bob。如果Bob控制超过50%的网络哈希算力，他可以继续挖他的私有欺诈区块链，直到它变得比诚实网络构建的分支更长。当区块a'+m+1被挖掘时（整数m>n），Bob可以公开发布他的欺诈分支，并且由于最长链规则，它将被识别为有效区块链。

## 条带式挖矿（Strip Mining）<sup>6</sup>

为了获得相对稳定的平均出块时间<sup>8</sup>，每当生成给定数量的区块<sup>7</sup>后网络难度会被调整。控制大量闲置网络哈希算力的攻击者可以非常快速地生成新区块。当达到难度调整高度时，网络难度将大大增加<sup>9</sup>，甚至提高到一个其他矿工几乎不可能成功挖矿的水平。此外，如果攻击者在难度重新调整后突然退出挖矿，则出块时间将急剧上升，从而有效地冻结网络，并导致大量未经确认的交易出现。

## 女巫攻击（Sybil Attack）

通过伪造大量假名身份，攻击者可以在点对点网络上获得不成比例的巨大影响力。某些节点可能仅连接到攻击节点，并与诚实网络隔离。这可以通过以下方式进一步利用 [11]。

一个攻击者可以：

1. 拒绝转发区块和交易。
2. 仅转发她自己的区块，从网络中分割出诚实节点。
3. 用0次确认过滤掉一些交易，例如，执行双花攻击（double spend attack）。
4. 通过观察来自诚实节点的传输并分析执行时间来执行定时攻击，从而威胁到区块链传输的低延迟加密和匿名性。

## 1.2 权益证明（Proof of Stake - PoS）

权益证明（PoS）是另一种流行的共识机制，其中矿工（或“权益持有者”）创建新区块的概率与该矿工所下注的权益额度成正比。PoS是一个一般概念，有不同实现方式。举个例子，权益可以是在所讨论的区块链上交易的相同加密货币的代币（例如，点点币（Peercoin），卡尔达诺（Cardano）），权益也可以是另一种形式的票（例如，德信币（Decred））。在一些实现中，所有代币都在区块链的创世区块中发行出来（例如，NXT，NEM）；在其它情况下，则不是（例如，Decred，Peercoin，NEO，Cardano）。

### 1.2.1 优点

PoS旨在解决PoW的一些缺点，包括成本、效率和易受中心化影响的问题。

---

<sup>6</sup> 感谢Alex Waters和Jonathan Silverman对基于PoW的区块链的漏洞进行评估。

<sup>7</sup> 在PAI币中，难度在每2,016个区块后重新调整。

<sup>8</sup> PAI币目标出块时间为10分钟。

<sup>9</sup> PAI币的网络难度在给定时间内可以改变不超过4倍。



PoS尝试使用安全保证金来激励参与者遵守网络规则，而不是大量的算力。参与者在提交一笔加密货币作为保证金后才能提议或验证区块。如果参与者试图欺骗网络，他们将失去部分或全部保证金。通过消除对计算资源的需求，PoS能够在显著降低能耗的同时维持网络安全。

在基于PoS的区块链中，出块时间可以设置为比基于PoW的区块链<sup>10</sup>低得多的水平，因为安全性不依赖于计算难题的难度。通过降低区块时间，基于PoS的区块链可以降低确认延迟，并且支持更高的每秒交易量。

在基于PoS的区块链中，将权益持有者的区块添加到区块链的概率与其使用的加密货币的数量成正比。可以说PoS是（a）更有效，更少浪费，因为它进行交易确认是不依赖于计算资源的，（b）由于准入门槛较低，更能抵抗中心化，因此（c）最终提供的解决方案比PoW更适合可持续的去中心化。

## 1.2.2 攻击向量和漏洞

### Nothing-at-Stake攻击

在PoW中，矿工被激励在单个（最长）链上挖矿，因为同时跨多个链的挖矿需要大量计算成本。而在PoS中，挖矿的计算成本是不存在的。因此，给定多个区块链分支时，最佳的（贪婪的）策略是同时对所有分支进行投票，这样无论分支的结果如何，验证者都可以得到奖励。

这种攻击务实地假设所有矿工都是贪婪的，会在每一条分支上行动，而且不是无偿行动。在这样的假设下，即使只占总权益的1%，当其他人都在所有分支下注时，攻击者的双花（double-spent）分支还是会赢。如果网络中有一些利他的矿工，攻击者则可能不得不购买更多的权益或贿赂其他验证人，但通过Nothing-at-Stake进行双花攻击仍然比在PoW中进行要相对容易。

已被提出的一些减轻Nothing-at-Stake攻击影响的方法：

- Ethereum Slasher 1.0用的是一个基于保证金的PoS算法；如果一个矿工在多条分支上投票，保证金就会被拿走 [12]。
- Ethereum Slasher 2.0惩罚投票给错误分支的投票者而不是惩罚进行双投的投票者 [1]。

---

<sup>10</sup>以太坊出块时间为15秒，比特币为10分钟

- 点点币 (Peercoin) 使用拥有最高耗币龄的链 (每个区块所获得下注的币总数乘以这些币下注后的时间之和)。
- NXT [27] 没有任何区块奖励, 仅靠交易费决定整个过程。
- 在EOS的委托权益证明 (Delegated Proof of Stake - dPoS) <sup>11</sup>中, 权益持有者将其权益下注到为区块生产者进行投票的过程当中 - 验证人的数量是固定的, 而且顺序在每轮决定。
- 在Algorand [28] 中, 账号 / 节点是随机选择的, 概率与持有的币成比例, 通过加密分选过程组成委员会。然后委员会使用BFT共识方法来产生区块。
- 混合PoW / PoS共识试图通过将PoW和PoS捆绑在一起消除PoW和PoS的缺点。

## 1.3 混合工作量证明与权益证明 (PoW/PoS)

PoW和PoS的缺点促使我们探索更安全的链上共识替代方案。混合PoW / PoS的特性使其成为潜在的候选方案。例如, 混合PoW / PoS提供以下功能:

- PoW矿工和PoS验证者相互依赖而带来的针对多数攻击更好的保护。
- 更低的网络参与准入门槛。
- 更高的能源效率。
- 由附带利益带来的更高网络稳定性, 例如维护节点始终在线的激励。

混合PoW / PoS有多种实现方式。受到Decred[14] (DCR) 的活动证明 (Proof of Activity) [15] 的启发, 我们提出以下设计方案。

### 1.3.1 概述

顾名思义, 混合PoW / PoS共识机制有两个主要组成部分: PoW挖矿和PoS区块投票。PoW矿工负责生产和提交新的候选区块。PoS权益持有者通过投票确认将候选区块附加到当前区块链。一个网络节点可以是PoW矿工, PoS权益持有者, 或两者同时。

PoW挖矿用经典的“中本聪”方式完成: 矿工不断生成随机数, 结合前一个区块的哈希和当前区块的默克尔根 (merkle root), 来生成不同的哈希值, 直到发现一个低于的阈值 (即目标, 动态改变) 的哈希值。

---

<sup>11</sup>由Dan Larimer在2013年发明。目前使用DPoS的区块链: EOS, BitShares, Steem, Golos, Ark, Lisk, PeerPlays, Nano (以前的Raiblocks) 和Tezos。部分基于DPoS的: Cosmos / Tendetmint, Cardano [13]。

在PoS部分中，权益持有者被随机选择对候选区块的有效性进行投票。一旦权益持有者的币被锁定了一段时间，即下注期，那么该权益持有者就成为新区块的潜在验证者。在每个区块高度，从所有潜在验证者中随机选择m个权益持有者为一组，被选择的概率与每个人下注的加密货币数量成正比。这些权益持有者将通过n-of-m投票决定新区块的有效性：如果多数验证者确认新区块的有效性，则该区块将被附加到区块链上。新区块包含所有m个权益持有者的投票以及权益发票。每个权益发票都列举了权益持有者<sup>12</sup>的下注额度，下注手续费和退还地址。它用于确认当前区块高度的下注活动。为了验证投票权益持有者的投票权，所有权益持有者的投票都会链接到一个先前记录在较低的区块高度的权益发票上。

区块奖励被分配给生产区块的PoW矿工、验证区块的m个权益持有者和/或其他方。具体分配方式是可调的。例如，在Decred中，60%分配给PoW矿工，30%分配给5个权益持有者（每人6%），10%分配给开发者。如果一名PoW矿工没有在候选区块中包含全部m次投票，则每错失一次投票奖励都将减少 $1/m$ 。

### 权益机制详情

假设Alice是一个PoS权益持有者，她想下注她的一些加密货币来对区块验证进行投票。

1. Alice向全网广播她愿意支付下注手续费来投入一定数量的加密货币。
2. PoW矿工（Bob）在区块高度为h时创建一个新区块，并将Alice的下注信息打包到权益发票中。下注手续费将被支付给Bob且不退还。Alice下注的加密货币则会被锁定。
3. Alice有资格在一个窗口期内投票，该时间窗口从区块h+256处开始并在区块h+256+W处结束。对每个由PoW矿工生成的候选区块，随机选择m个符合条件的权益持有者来验证该候选区块，被选的概率与下注的额度成比例。
4. 窗口期的长度W取决于全网所下注的权益，并且被设置成使Alice很有高的可能性在窗口期内被选为验证者。
5. 如果Alice，在窗口期内
  - a. 被选为验证者并在一个区块上投票
  - b. 被选，但离线因而错过投票的机会（即节点离线）
  - c. 未被选作验证者

她的资金（权益和区块奖励（如果有），减去下注手续费）在接下来的256个区块期间保持锁定状态，之后将被释放。

---

<sup>12</sup>可能是也可能不是投票的权益持有者。

### 1.3.2 技术参数

当前基于PoW的Project PAI和基于混合PoW / PoS共识机制的Decred区块链的技术参数比较如下表所示：

	Project PAI, 当前	Decred
哈希算法	SHA-256	BLAKE-256
总供应量	2100000000	21000000
目标出块时间	10分钟	5分钟
难度调整间隔	2016个区块 (2周)	144个区块 (1.25天)
区块奖励的递减比值	50/100	100/101
区块奖励递减的间隔	210000个区块 (4年)	6411个区块 (21天, 8小时)
区块奖励分配	100%给PoW矿工	60%给PoW矿工+ 30%给权益持有者 (每个6%) + 10%给开发团队
发行时间	2/23/2018	2/8/2016
预计挖矿寿命	到2154	到2120
创世区块后初始区块奖励	1500	31.19582664

表 1. Project PAI和Decred技术参数比较表

Decred是混合PoW/PoS区块链的一个例子。PAI币的开发人员正在研究最适合拟议的混合共识机制的参数集。

### 1.3.3 攻击向量和漏洞

#### 多数攻击

如1.1.2节所述，多数攻击本质上意味着攻击者可以比网络的其他节点更快地生成有效区块。在PoW中，控制超过50%的网络哈希算力足以获得这样的优势。但在混合PoW / PoS中，攻击不仅要控制网络哈希算力的一部分，还要控制网络总下注权益的一部分。

每个有效区块都需要包含来自PoS权益持有者的投票。控制大部分网络哈希算力的攻击者能比其他  
人更快地在本地私下生成候选区块。然而，一旦这个更长的私人链发布，PoS权益持有者将开始在  
处于分支处的区块上验证和投票，而不是在较长的私有链顶部。因为投票的权益持有者是根据他们  
持有多少权益的比例随机选择的，所以他们在理论上对PoW矿工来说是未知的。因此，除非攻击  
者控制大部分网络哈希算力和总下注权益，绝大多数攻击都不太可能发生。

声明：在3-of-5的PoS投票方案中，一个拥有占总下注权益比例  $f_s$  权益的攻击者需要同时拥有

$$\frac{6(1-f_s)^5-15(1-f_s)^4+10(1-f_s)^3}{6f_s^5-15f_s^4+10f_s^3}$$

倍的诚实网络的哈希算力来获得挖矿优势。证明请参见附录A。有关普遍投票方案的分析，请参阅  
[15]。

$\frac{\text{攻击者持有权益}}{\text{网络总权益}}$  和  $\frac{\text{攻击者哈希算力}}{\text{诚实网络哈希算力}}$  的关系如图2所示。例如，如果攻击者拥有约50%的  
总下注权益，他或她还需要100%的诚实哈希算力来跟上诚实链的出块速度

总体而言， $\frac{\text{攻击者持有权益}}{\text{网络总权益}}$  越大，进行一次多数攻击所需的  $\frac{\text{攻击者哈希算力}}{\text{诚实网络哈希算力}}$  的比值就越  
小。尽管购买或出售币总供应量的一大部分并不容易，但如果权益参与下降（例如，由于大型权益  
池离线或所有代币被挖），多数攻击可能就会引起关注。一般而言，混合系统保持高权益参与是非  
常重要的。有关混合共识系统下的Project PAI多数攻击成本分析，请参见附录B [17]。

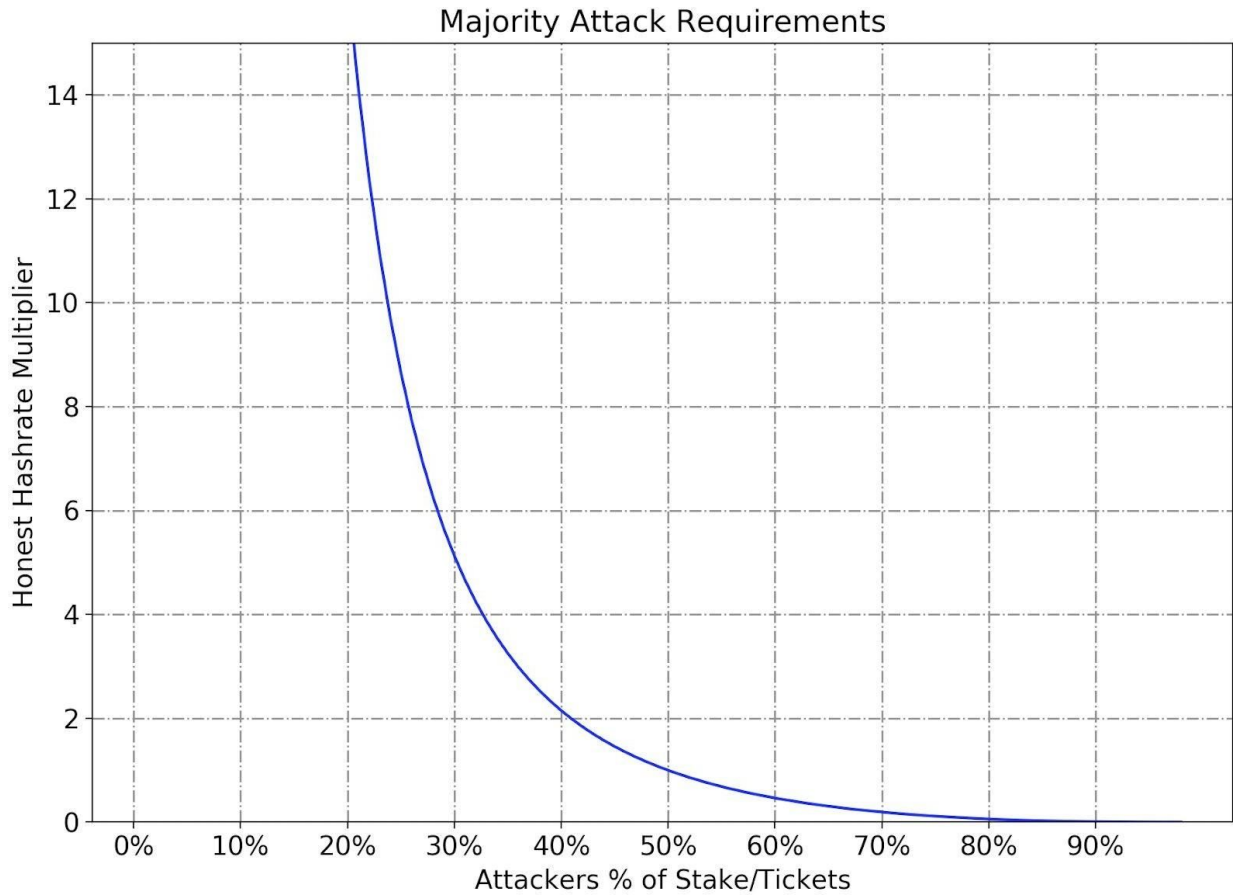


图 2. 跟上诚实链出块速度所需的PoW和PoS比例

### Nothing-at-Stake攻击

如果矿工挖到一个尝试产生分支的恶意区块，验证者可以简单地拒绝该区块。由于PoW挖矿部分本就需要一些计算成本，矿工们没有动力去为了一条不会被验证者批准的分支而费力的。同样，由于权益持有者已经预先为投票的权利下注，他们会倾向于以期待中别的投票者将来会投票的方式来投出自己的票（即最长链，因为其最有可能产生区块奖励），而不是在其他分支上浪费机会。

### 权益池

参与混合系统的PoS投票部分要求验证者的钱包软件不间断运行。钱包需要保持在线才可能随时被调用来投票 - 如果钱包不可用，将失去投票机会且无法收到任何区块奖励。

无法保持钱包在线的权益持有者可以将投票权委托给权益池。通过1-of-2多重签名（multisig），用户能够将自己的投票权授予权益池，而无需授予权益本身的访问权。

遗憾的是，中心化的权益池会受到单点故障的影响。持有太多投票权的权益池有可能会强行通过或否决某一区块。此外，如果一个大型权益池离线，大量的投票可能因此流失，从而导致撤票。所以通常会建议使用较小的权益池 [20]。

### 1.3.4 其他好处

如上所述，混合系统的PoS机制要求钱包软件不间断运行，以防权益持有者错失投票机会。此外，由于区块奖励被分配给PoW矿工和PoS权益持有者，因此混合机制中的PoW挖矿部分通常比纯PoW挖矿利润更低。所以参与节点可以投入较少的资金来获得哈希算力，从而降低新PoW矿工进入的门槛。这两个因素都有助于促进更高的网络参与度。最后，由于减少了潜在的对哈希算力的总投资，网络能耗可能相对低于纯PoW。

在经典PoW中，矿工会组成了中心化的算力池，来提高他们赢得区块的机会。一个矿池拥有的哈希算力越多，该矿池就越有可能赢得区块奖励，从而吸引更多节点入池（即马太效应 [30]）。相反，在混合PoW / PoS中，权益池的存在仅仅是为了让钱包在线，这样验证者才不会错过投票机会。权益池规模对一个持有者被选中的机会没有影响。虽然混合PoW / PoS仍然可能导致形成大型中心化的算力矿池，但由于PoS层能提供额外的安全性，受其影响程度较低。总而言之，混合PoW / PoS的中心化程度预计低于传统PoW。

## 第2节——工作量证明（PoW）的哈希函数

选择工作量证明所用哈希函数的目的是通过自然公平的公共挖矿<sup>13</sup>帮助促进真正的去中心化。理想的候选加密哈希函数具有以下属性 [21]：

1. 确定性 - 相同的输入信息总是产生相同的哈希输出
2. 高效性 - 能很快地由从任何给定输入信息计算哈希输出
3. 安全性 - 无法由哈希输出高效生成输入信息，只能使用暴力求解算法

---

<sup>13</sup>感谢Tamover LLC的Jascha Wanger为关于不同共识机制对网络安全性，性能和采用的影响提供了全面概述。

4. 随机性 - 输入信息的微小变化导致哈希输出发生的大量不相关变化
5. 唯一性 - 无法找到具有相同哈希输出的两个不同输入信息

满足上述标准的哈希函数被认为是密码学安全的。此外，在许多情况下，如果底层哈希函数是抗ASIC（Application-Specific Integrated Circuit）的话，它就被认为是区块链的理想选择，即，与基于CPU的矿机相比[22]，通过在ASIC上实现该算法，无法显著的计算加速。请注意，虽然ASIC可抗性（*ASIC resistance*）是理想的，但从长远来看实际上是不可能实现的（详见“ASIC可抗性”部分）。

有关不同加密货币采用的哈希函数，请参阅附录C。

SHA-3[31]哈希函数族具有一系列有利的性质，其中包括<sup>14</sup>:

- 与MD结构的哈希算法（MD5, SHA-1, SHA-2）相比有更好的时间效率
- 更高的能效：对于相同的难度水平，计算消耗（消散）更少的能量（热量）
- 密码学安全性：在可见的将来一段时间内，在SHA-3（或SHA-2）上发现任何经典或量子攻击的可能性极小
- ASIC可抗性：ASIC目前尚未被广泛使用

有关所讨论的混合PoW / PoS共识机制的PoW组成部分，本提议建议考虑SHA3-256，以及SHA-3的变体SHAKE-256 [31]，它具有类似的安全性，但更高效，且支持可变的输出长度。

## 2.1 ASIC可抗性

附录C中提到的一些哈希算法是专门为ASIC可抗性设计的。Scrypt和Cryptonight占用大量内存，缩小了ASIC挖矿和CPU/GPU挖矿之间的差距；X11使用一系列科学哈希算法（十一种），增加了研发一个ASIC矿机所需的成本；X16R也使用哈希算法序列，另外还会定期打乱哈希算法的排序。尽管有这些方式，但只要市场上有足够的经济激励，针对理想上抗ASIC哈希算法的ASIC矿机还是会被研发出来（例如，Scrypt和Cryptonight）。

---

<sup>14</sup>感谢加州理工学院的Thomas Vidick教授为此处考虑在内的许多哈希函数提供了的评估和总结以及总体建议。

<sup>15</sup>Monero（XMR）建议定期改变哈希算法（每年两次）来淘汰现有ASIC矿机。



事实上，人们甚至质疑是否有100%完全抗ASIC哈希算法<sup>15</sup>存在。此外，关于是否真的有必要与ASIC矿机作抗争 [23] 也存在着争议。为了以最低的风险开放挖矿，更合理的方法可能是寻找一个当前只有极少数现有ASIC挖矿针对的哈希函数（如果其存在的话），并与混合工作量证明（Proof-of-Work - PoW）／权益证明（Proof-of-Stake - PoS）共识机制结合使用。加州理工学院的Vidick教授强烈建议“不要将SHA-3作为独立工作量证明的一部分使用，而是结合其他方法，如权益证明，以减少51%攻击的可能性。”

## 第3节——建议与未来工作

### 3.1 总体建议

- SHA-3的有利属性使其成为混合PoW／PoS共识机制中PoW部分的良好候选算法。建议使用SHA3-256和SHA-3的变体SHAKE-256。
  - 虽然使用任何哈希函数都可能难以实现长期的ASIC抗性，但用一种暂无ASIC矿机存在的算法来取代PAI币当前使用的SHA-256算法可以提供短期保护。而SHA-3是满足这个条件的。
- 通过将SHA-3变体与混合PoS / PoW算法配对，可以实现针对51%攻击的长期保护。第1.3节中概述的方法通过要求PoW矿工和PoS验证者之间互相依赖来应对PoW和PoS各自的缺陷。
- 基于上述研究和对现有技术的回顾，总体建议是Project PAI采用混合PoW / PoS共识机制。这种机制应该结合使用SHA-3变体与第1.3节中所概述的混合共识机制。

### 3.2 未来工作

随着PAI币开发人员的研究和开发工作展开，将会有更多有关PAI币代码库集成和部署的技术细节公布。

## 附录A——多数攻击的数学论证

一个拥有占总下注权益比例  $f_s$  权益的攻击者需要同时拥有  $\frac{6(1-f_s)^5-15(1-f_s)^4+10(1-f_s)^3}{6f_s^5-15f_s^4+10f_s^3}$  倍的诚实网络的哈希算力来获得挖矿优势

论证:

1. 样本空间  $E_1 = \{3\text{张或更多投票被攻击者控制}\}$ ; 样本空间  $E_2 = \{3\text{张或更多投票被诚实权益持有者控制}\}$ ; 样本空间  $E_3 = \{5\text{名投票者在线}\}$
2.  $Pr[E_1 | E_3] = C_5^5 * f_s^5 + C_5^4 * f_s^4 * (1 - f_s) + C_5^3 * f_s^3 * (1 - f_s)^2 = 6f_s^5 - 15f_s^4 + 10f_s^3$
3.  $Pr[E_2 | E_3] = 6(1 - f_s)^5 - 15(1 - f_s)^4 + 10(1 - f_s)^3$
4. 平均而言, 攻击者将在  $\frac{1}{Pr[E_1 | E_3]}$  次随机nonce尝试后生成一个区块; 诚实网络需要  $\frac{1}{Pr[E_2 | E_3]}$  次尝试
5. 如果诚实网络每进行一次随机nonce尝试的同时, 攻击者可以进行  $\frac{Pr[E_2 | E_3]}{Pr[E_1 | E_3]}$  次尝试, 攻击者便能够以与网络其他节点相同的平均速度来生成区块

## 附录B——多数攻击的成本分析

我们用攻击Project PAI混合共识的两个部分来估算攻击成本：（1）PoS中购买币下注的成本，以及（2）PoW中获取GPU算力的成本。我们定义：

$$\text{权益比} = \frac{\text{攻击者持有权益}}{\text{网络总下注权益}}$$
$$\text{诚实哈希算力倍数} = \frac{\text{攻击者哈希算力}}{\text{诚实网络哈希算力}}$$

我们假设诚实矿工拥有100个NVIDIA TESLA V100 GPU，截至2018年12月17日，每个价值为6369美元 [29]。它们代表诚实哈希算力的最小值。表2显示了截至2018年12月17日的统计数据的攻击成本：

PAI币的币值: 0.052201美金  
币的总供应量: 1563172500  
公开可购买的币供应量: 735000000

权益比 (%)	占公开可购买的币供应量百分比 (%)	币的购买成本 (百万美元)	诚实哈希算力倍数	GPU算力的获得成本 (百万美元)	总攻击成本 (百万美元)
18.93	40.25	15.44	19	12.09	27.54
24.66	52.45	20.13	9	5.73	25.86
28.99	61.66	23.66	5.67	3.6	27.26
32.66	69.46	26.65	4	2.55	29.2
35.94	76.44	29.33	3	1.91	31.24
38.98	82.91	31.81	2.33	1.48	33.29
41.86	89.02	34.16	1.86	1.18	35.33
44.63	94.91	36.41	1.5	0.95	37.36
47.33	100.66	38.62	1.22	0.78	39.4
50	106.34	40.8	1	0.64	41.44

52.67	112.02	42.98	0.82	0.52	43.5
55.37	117.77	45.19	0.67	0.42	45.61
58.14	123.66	47.44	0.54	0.34	47.78
61.02	129.77	49.79	0.43	0.27	50.06
64.06	136.23	52.27	0.33	0.21	52.48
67.34	143.22	54.95	0.25	0.16	55.11
71.01	151.02	57.94	0.18	0.11	58.05
75.34	160.22	61.47	0.11	0.07	61.54
81.07	172.43	66.16	0.05	0.03	66.19

表 2. 攻击成本表

请注意，占公开可购买的币供应量百分比大于100%的所有行都代表不可能进行多数攻击的情况。

在0.05美元的PAI币价格点上，当攻击者控制着从5%到95%的网络哈希算力并且有足够公开可购买币供应量来取得所需权益比时，总攻击成本从2586万美元到6619万美元不等。

图3显示了攻击基于纯PoW的PAI币网络和基于混合PoW / PoS的PAI币网络的成本之间的比较。

购买币的成本与PAI币价值呈线性关系。当PAI币价值为0.25美元时，以18.93%的权益比和95%的网络哈希算力进行多数攻击的总成本是8605万美元，当PAI币的价值为1.00美元时，则为3.0793亿美元。

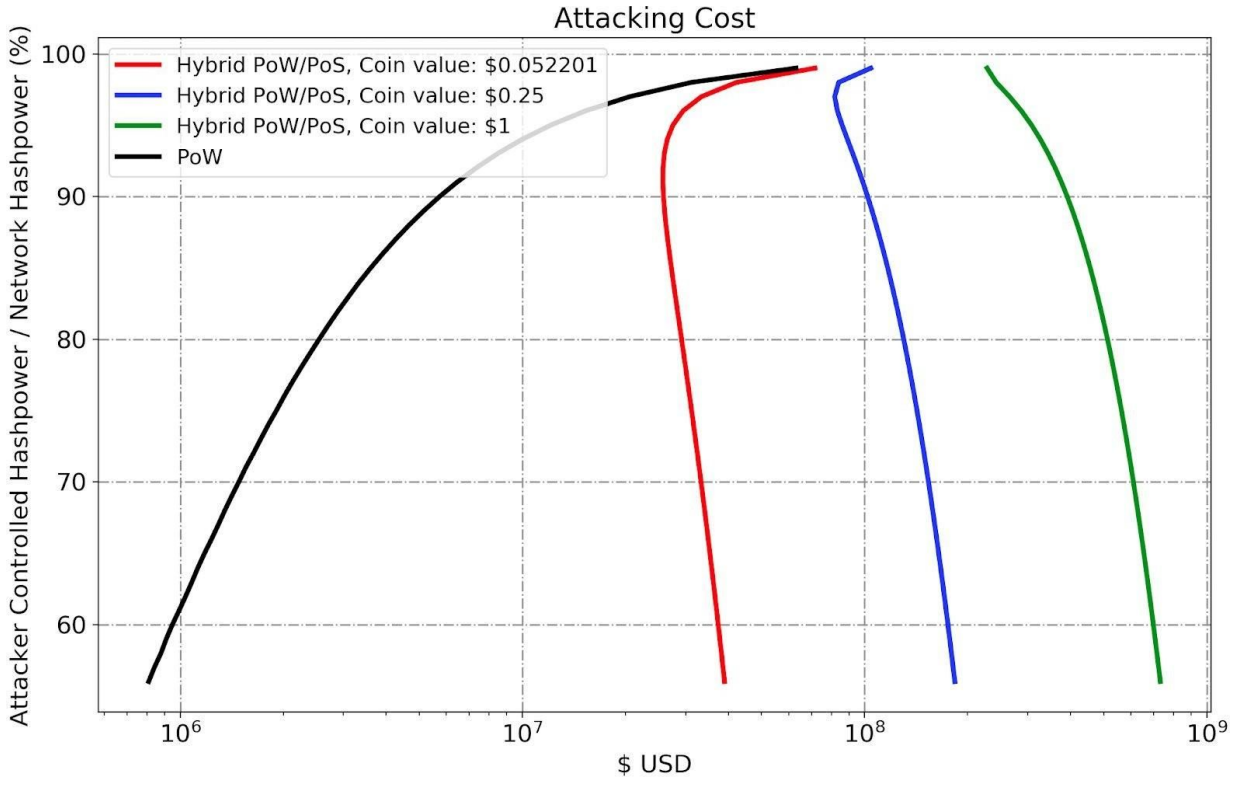


图3. PoW和混合PoW / PoS的攻击成本

## 附录C——加密货币的哈希算法

哈希算法	哈希算力	加密货币	现有ASIC矿机
SHA-256	GH/s	Bitcoin Cash (BCH), Bitcoin (BTC), 21Coin (21), Peercoin (PPC), Namecoin (NMC), Unobtanium (UNO), Betacoin (BET), Bytecoin (BTE), Joulecoin (XJO), Devcoin (DVC), Ixcoin (IXC), Terracoin (TRC), Battlecoin (BCX), Takeicoi (TAK), PetroDollar (P\$), Benjamins (BEN), Globe (GLB), Unicoi (UNIC), Snowcoi (SNC), Zetacoi (ZET), Titcoi (TIT)	Antminer S9, Antminer T9
Scrypt	KH/s	Litecoin (LTC), Dogecoin (DOGE), Novacoin (NVC), WorldCoin (WDC), Latium (LAT), FeatherCoin (FRC), Bitmark (BTM), TagCoin (TAG), Ekrona (KRN), MidasCoin (MID), DigitalCoin (DGC), Elacoin (ELC), Anoncoin (ANC), PandaCoins (PND), GoldCoin (GLD)	Antminer L3
Cryptonight	H/s	Monero (XMR), Bytecoin (BCN), Boolberry (BBR), Dashcoin (DSH), DigitalNote (XDN), DarkNetCoin (DNC), FantomCoin (FCN), Pebblecoin (XPB), Quazarcoin (QCN)	Antminer X3
Dagger Hashimoto (Ethash)	MH/s	Ethereum (ETH), Ethereum Classic (ETC), Expanse (EXP)	Antminer E3
Equihash	MH/s	Zcash	Antminer Z9
X11 (X13, X15, X17)	MH/s	Dash (DASH), CannabisCoin (CANN), StartCoin (START), MonetaryUnit (MUE), Karmacoin (Karma), XCurrency (XC)	Antminer D3
X16R		Ravencoin, Motion(XMN)	
BLAKE-256 (BLAKE2s)		Decred	iBeLink DSM 6T, iBeLink DSM 7.2T, Innosilicon D9, Ffminer DS 19
SHA-3 (Keccak)		MaxCoin (MAX), Slothcoin (SLOTH), Cryptometh (METH), NEM	

# References

- [1] Foundation, Ethereum. "Proof of Stake: How I Learned to Love Weak Subjectivity." *Ethereum Blog*, [blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/](http://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/).
- [2] "Decentralized Application." Wikipedia, Wikimedia Foundation, 2 Dec. 2018, [en.wikipedia.org/wiki/Decentralized\\_application](http://en.wikipedia.org/wiki/Decentralized_application).
- [3] "Peer-to-Peer." Wikipedia, Wikimedia Foundation, 13 Dec. 2018, [en.wikipedia.org/wiki/Peer-to-peer](http://en.wikipedia.org/wiki/Peer-to-peer).
- [4] "Whitepaper." Project PAI, 13 Nov. 2018, [projectpai.com/assets/files/whitepaper/whitepaper-tech.pdf](http://projectpai.com/assets/files/whitepaper/whitepaper-tech.pdf).
- [5] Projectpai. "Projectpai/Pdps." GitHub, [github.com/projectpai/pdps/blob/master/pdp-0002.mediawiki](https://github.com/projectpai/pdps/blob/master/pdp-0002.mediawiki).
- [6] "About | ObEN, Inc." ObEN Inc, [oben.me/about-us-3/](http://oben.me/about-us-3/).
- [7] "S2 Server Manual." BITMAIN, [file.bitmain.com/shop-bitmain/download/Antminer%20S2%20Manual\\_EN.pdf](http://file.bitmain.com/shop-bitmain/download/Antminer%20S2%20Manual_EN.pdf).
- [8] Projectpai. "Projectpai/Paicoi." GitHub, [github.com/projectpai/paicoi/blob/master/src/coinbase\\_addresses.h](https://github.com/projectpai/paicoi/blob/master/src/coinbase_addresses.h).
- [9] Projectpai. "Projectpai/Paicoi." GitHub, [github.com/projectpai/paicoi/blob/master/src/validation.cpp#L2793](https://github.com/projectpai/paicoi/blob/master/src/validation.cpp#L2793).
- [10] AndrewMarshall. "Proof-of-Work (PoW). All about Cryptocurrency - Bitcoin Wiki." . What Is Blockchain Technology? - Bitcoin Wiki, Bitcoin Wiki, 22 Oct. 2018, [en.bitcoinwiki.org/wiki/Proof-of-work#The\\_advantages\\_of\\_PoW](http://en.bitcoinwiki.org/wiki/Proof-of-work#The_advantages_of_PoW).
- [11] "Weaknesses." B-Money - Bitcoin Wiki, [en.bitcoin.it/wiki/Weaknesses#Sybil\\_attack](http://en.bitcoin.it/wiki/Weaknesses#Sybil_attack).
- [12] Foundation, Ethereum. "Slasher: A Punitive Proof-of-Stake Algorithm." Ethereum Blog, [blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/](http://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/).
- [13] Myles Snider, Kyle Samani, and Tushar Jain. "Delegated Proof of Stake: Features & Tradeoffs." Multicoi Capital, [multicoi.capital/wp-content/uploads/2018/03/DPoS\\_-Features-and-Tradeoffs.pdf](http://multicoi.capital/wp-content/uploads/2018/03/DPoS_-Features-and-Tradeoffs.pdf)
- [14] "Decred - Autonomous Digital Currency." Decred - Autonomous Digital Currency, [www.decred.org/](http://www.decred.org/).
- [15] Bentov, Iddo, et al. "Proof of Activity." ACM SIGMETRICS Performance Evaluation Review, vol. 42, no. 3, Aug. 2014, pp. 34–37., doi:10.1145/2695533.2695545.
- [16] Decred. "Decred/Dcps." GitHub, [github.com/decred/dcps/blob/master/dcp-0001/dcp-0001.mediawiki](https://github.com/decred/dcps/blob/master/dcp-0001/dcp-0001.mediawiki).
- [17] Zia, Zubair. "Decred's Hybrid Protocol, a Superior Deterrent to Majority Attacks." Medium.com, Medium, 4 July 2018, [medium.com/decred/decreds-hybrid-protocol-a-superior-deterrent-to-majority-attacks-9421bf486292](https://medium.com/decred/decreds-hybrid-protocol-a-superior-deterrent-to-majority-attacks-9421bf486292).
- [18] "Defence Against Early Stage Botnet Attack?" Decred Forum, [forum.decred.org/threads/defence-against-early-stage-botnet-attack.84/](http://forum.decred.org/threads/defence-against-early-stage-botnet-attack.84/).
- [19] "How to Stake/Vote." Decred Documentation, [docs.decred.org/mining/how-to-stake/](http://docs.decred.org/mining/how-to-stake/).

- [20] "Voting Service Providers." Decred Documentation, docs.decred.org/faq/proof-of-stake/stake-pools/.
- [21] "Cryptographic Hash Function." Wikipedia, Wikimedia Foundation, 9 Nov. 2018, en.wikipedia.org/wiki/Cryptographic\_hash\_function.
- [22] "What Does It Mean for a Cryptocurrency to Be ASIC-Resistant?" Bitcoin Stack Exchange, bitcoin.stackexchange.com/questions/29975/what-does-it-mean-for-a-cryptocurrency-to-be-asic-resistant.
- [23] Hsue, Derek. "Is The War Against ASICs Worth Fighting? – Token Economy." Token Economy, Token Economy, 4 Apr. 2018, tokeneconomy.co/is-the-war-against-asics-worth-fighting-b12c6a714bed.
- [24] Dexter, Shawn. "Understanding Longest Chain – A Simple Analogy." Mango Research, 9 Sept. 2018, www.mangoresearch.co/understanding-longest-chain-rule/.
- [25] "Unspent Transaction Output, UTXO." FAQ - Bitcoin, bitcoin.org/en/glossary/unspent-transaction-output.
- [26] Sunny King, Scott Nadal. "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake." peercoin.net/assets/paper/peercoin-paper.pdf.
- [27] Nxt Community. "Nxt Whitepaper." dropbox.com/s/cbuwrorf672c0yy/NxtWhitepaper\_v122\_rev4.pdf.
- [28] "Whitepapers." Algorand, algorand.com/docs/whitepapers/.
- [29] "Nvidia Tesla v100 16GB." Amazon, Amazon, www.amazon.com/PNY-TCSV100MPCIE-PB-Nvidia-Tesla-v100/dp/B076P84525.
- [30] "Matthew Effect." Wikipedia, Wikimedia Foundation, 21 Nov. 2018, en.wikipedia.org/wiki/Matthew\_effect.
- [31] SHA, NIST. "standard: Permutation-based hash and extendable-output functions, 2015." (3).





