

Kleros

黄皮书 v2.0.2

Clément Lesaege, William George, 和 Federico Ast

2021 年 7 月

摘要

Kleros 为智能合约平台专属的去中央化决策协议，而目前其已被积极导入于以太坊生态系统。Kleros 主要功用为运作以一去中央化第三者来为一系列简单至复杂之问题提供正确解答输出。为达成此目的，Kleros 运用精密经济博弈论来使系统内的众招陪审员能依据规范来做出正确决策。基于以上介绍，Kleros 欲以一经济实惠，可信赖，快速，及去中央化的方式来提供决策判断。其中一主要用途为被使用做为争议解决协议，并创建一真正的去中央化型正义。

1 介绍

“治法同于治国”。Aristotele。

世界正经历一急速变化的全球化及数位化。而前所未见的庞大交易量正被执行于网路数位平台横跨各法治管辖区域。如区块链科技确实不负众望达成其开发潜力，多数物资，劳力，及资本将被运用于去中央化平台于不久未来。随其平台利用成长，争议纠纷也必然升增。去中央化版本的 eBay 用户将宣称贩卖者失败来确实履行传送合约指定的物资，去中央化 Airbnb 的用户将抱怨订租房间与合约中图片不符，而去中央化众筹平台的资助者将与资助之开发团队间产生争议如其无法提交合约保证之开发成果。

智能合约能完全依照其所设计之程式来进行运作，但其无法自主进行客观判断或来获取任何区块链外资讯。既有之争议解决方案极为慢旧，且非常昂贵及不可靠来使区块链经济来及时有效地运作于此建立基础之上。区块链的新经济时代需要一快速，实惠，公开，可靠，及去中央化争议解决机制来为智能合约们提供最终正确判断。

Kleros 为一决策协议，其运用多目的法庭系统来解决各类争议。此为一被部署至以太坊的自主组织，并运作为一去中央化第三者来仲裁¹争议为各类从极简至复杂设计之合约。仲裁的各步

¹ 于此，“仲裁”一词于此被用于一非正式意涵。Kleros 决策被用于既存法律系统的状态可能性为一目前重点研究方向。

骤(确保证据, 选择陪审员, 等等) 将被完全自动化。Kleros 不依赖一集中单体的诚实可靠性, 反之, 其依赖经济博弈论的群体人性激励机制。

此设计基础上基于一法治知识论观点: 一法庭为一重要知识泉源, 而其也为一工具来从模糊证据中辨别真相。一参与者(陪审员)遵照一系统之规范程序来使输入资讯(证据)能被用于生成一相当输出资讯(决策) [42]。Kleros 利用并提升众招技术, 区块链科技及博弈理论来开发一能以经济实惠及安全可靠的方式来提供真实决策的正义系统²。

2 先前研究成果: Schelling Point(谢林点)机制

博弈论学者 Thomas Schelling 开发一聚焦点/Schelling Point (谢林点)概念[55]来作为一方案使群众能同调行动即便于无法沟通之情况下³, 其原理主要依赖于抉择通常将倾向于最自然且最相关的选项。Schelling 解释此概念利用以下范例: “如您明天必须与一陌生人见面于纽约, 何时及何地您将尝试来见他?”。虽几乎所有场所及地点几乎都能成为可能回答选择, 多数常见回覆将倾向“纽约中央车站, 中午十二点”。此似乎无一具体原因来使中午十二点的纽约中央车站能成为一高人气选项(其他所有场所及时间看起来都可行来提通参与者来进行协调), 但因传统见面习性, 中央车站自然成为一合理聚焦点。

基于谢林点的基础概念, 以太坊创建者 Vitalik Buterin 曾提议谢林币[15]的创建提案, 其主要概念为一代币能利用经济性诱因机制来提供真相。如我们欲想知道巴黎是否真于昨天下雨, 我们能问各谢林币持有主”请问昨天巴黎是否真下雨? 请选择是或否”。各代币持有主将能透过一秘密选票函来投票, 而所有投票完成后, 此结果将被公开。投票与多数决同调决议的参与者将获得原先持有代币量的 10%增量奖励。而与多数决不同调决议的参与者将损失 10%的原先代币持有量。

Thomas Schelling [55] 形容“聚焦点(们)为每个人对于群众对其预测所做出之预测的预测”。谢林币使用此机制为轴心来提供诱因至无法互相信任及认识的系统参与者。我们期盼参与者将选择正确选项作为最终决策因其期盼他人也将会如此行事且做出此正确决策, 因其期盼他人也将会如此行事且做出正确决策... 于此简单范例, 谢林点为确实诚实可靠。

² 为提供判断基础观点来决定拟-Kleros 科技系统是否能被视为提供”去中央化正义”, 详细请参照[7]。

³ 值得注意的是, Schelling 点机制运用于区块链将几乎无法保证参与者确实无法互相沟通因其通常执行于拟-匿名环境。而于 Kleros 案例, 我们将发现 Kleros 具有一上诉系统来激励参与者将还未发生的可能上诉机会也纳入考量, 而其部分添增回复沟通非可能性特质。此外, 我们将更加深入研究如何激励参与者来不信任任何可能之相互间沟通, 而 [28] 研究争论即便此情况使发生, 谢林点还是会依旧存在发生, 详细请查看 4.9 章节。

The majority votes \ You vote	You vote	
	YES	NO
YES	+0.1	-0.1
NO	-0.1	+0.1

图 1：基本谢林博弈的收益表

谢林币机制已被运用于多数去中心化预言机数据提供及预测市场 [59] [49] [3]。我们注意到目前专注于 Kleros 的学术研究也正目前尝试来使用此机制于争议解决⁴ [21]。而此最基本的共识为符合多数的正确投票必须确实被系统适当激励。Kleros 的基础激励设计建立于一类似谢林币的形式之上，并进行些微调整来使回答能针对部分挑战包含扩张性，客观性，及隐私性来使参与者能确实以适当行为来进行参与。

3 使用范例

Alice 为一创业家于法国。她雇用 Bob，一瓜地马拉来程式设计师，于一 P2P 自由职业平台来为她公司建立一新网站。于同意计价及相关服务合约条款后，Bob 开始正式工作。数星期后，Bob 提交其完成产品。但接收成品后，Alice 极度不满因为 Bob 的工作成果品质比预期中低许多。但 Bob 回覆其完全按照合约所示来建立产品。Alice 非常沮丧，她无法有效率的雇用一律师来为一仅价值数百美金的案例，更不用说 Bob 住在地球遥远的另一端。

假设 Alice 和 Bob 先前使用 Kleros 第三方托管服务并明确指出于合约中如双方间争议产生，其将被 Kleros 法庭来做判决，则此情况将究竟变的如何呢？当 Bob 开始无视 Alice 的抱怨信件后，Alice 将按下一“传送至 Kleros”按钮，并填入基本案件叙述来简单解释情况。

千里之外，于肯尼亚内罗毕，Chief 为一名软体开发员。于其”空闲”时间座车去上班的时候，他查看 Kleros 法庭官网(<https://court.kleros.io>) 来寻找争议来帮忙解决工作。他平均每年赚取数千美金藉由当陪审员来解决发生于网上雇用的软体设计师及其雇主间的任何争议。Chief 通常于”网站品质”一庭来进行审议判决。此法庭需要 html，javascript，及网站设计的相关知识来足以正确解决客户及雇主间的争议。Chief 质押 2000 PNK，一代币被 Kleros 用来选择争议陪审员。如质押代币数量越多，其被抽选为陪审员的机率越高。假设 Chief 将为争议做出正确审议，其质押之 2000 PNK 及添增之仲裁奖励费将会被全权归还给他，详细请查看 4.7.3 章节。

⁴ 相较于 Kleros，提案 [21] 使用一不同架构来决定仲裁者质押如何被选择，投票，及接着获得争议费用，主要利用一添增“验证”期间的谢林游戏机制。另一他值得注意的变化差异为，虽然提议 [21] 不包含一用来预防 51% 攻击的法庭树结构机制形容于章节 4.3，其确实包含一新“论坛”提案来使社群成员能被激励来不仅能贡献远超于正确投票，其也能被激励来进行提案为治理或任何其他新合约模组。

约一小时过后，一电邮进入 **Chief** 信箱：“您已被选为一陪审员为一网站设计争议。请下载证据于此。您有共计三天时间来完成提交最终决策。”类似电邮也被位于秘鲁克斯库的程式设计师 **Benito**，及罗马尼亚的 **Alexandru** 所接收，他们也同时正质押 **PNK** 于“网站品质”法庭上。此三人随机被从一 3000 人的陪审员池中选出。他们将很有可能永远不会互相认识，但他们将会合作协力来协助仲裁 **Alice** 和 **Bob** 的争议。于回家的巴士中，**Chief** 研究争议证据并投票决策谁对谁错。

两天过后，当三名陪审员确实投票后，**Alice** 及 **Bob** 接收至一电邮：“陪审员已决议倾向 **Alice** 方。网站设计确实不符合双方先前于合约中同意之服务条款。一智能合约已传送资金回至 **Alice**”。陪审员接着被奖励于其贡献，并最终结案。

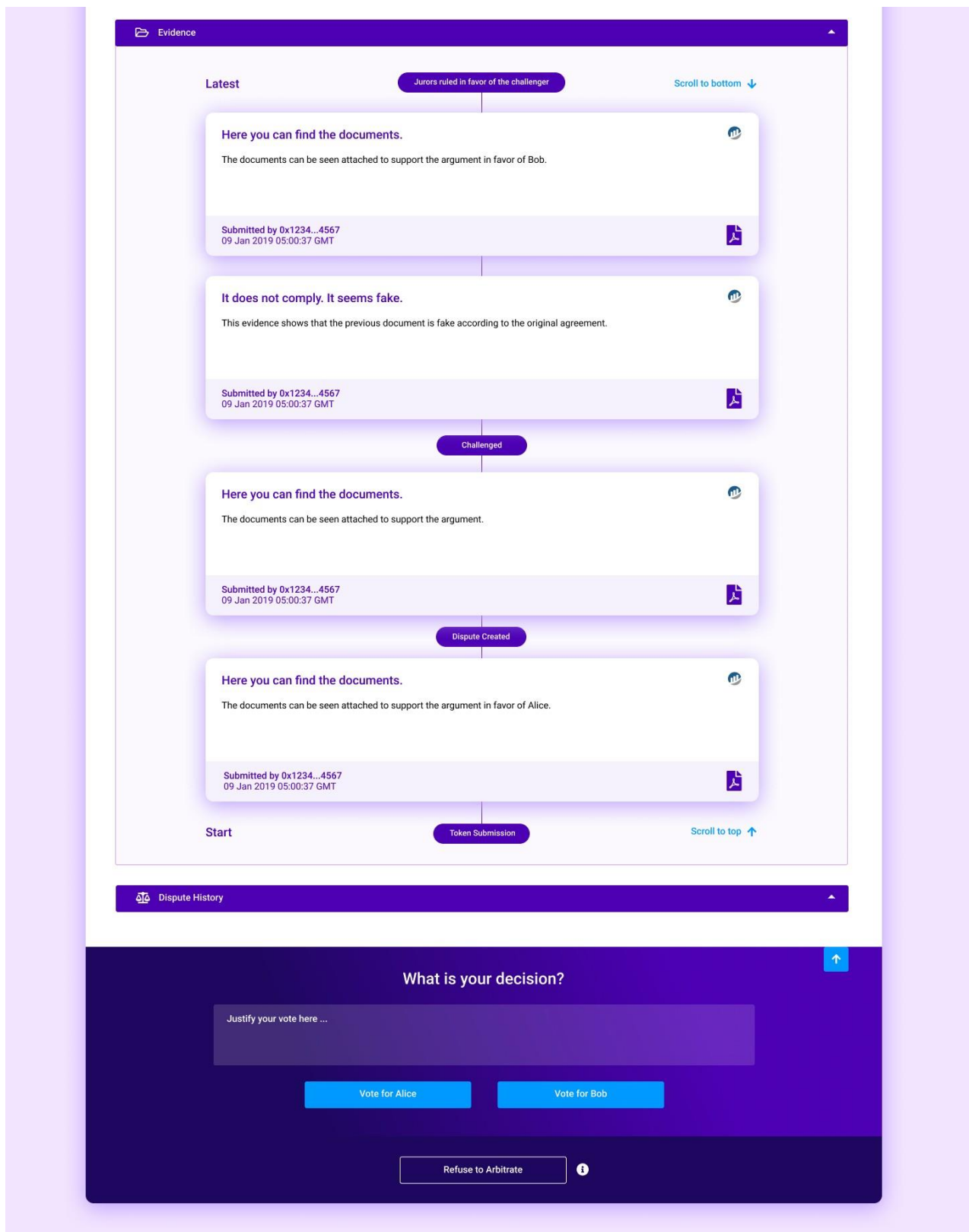


图 2：于陪审员做出决策当下显示之证据

4 Kleros 机制设计

于此章节，我们将详细讨论 Kleros 设计架构⁵。

4.1 可仲裁方及仲裁方合约

Kleros 为一插件型法庭系统。“被仲裁”及“可被仲裁”方之智能合约经需要选择 Kleros 为其仲裁方。当插件与 Kleros，合约创建主将决定陪审员人数及其归属法庭为此合约案例，详细请查看 4.3 章节。Kleros 团队已开发一系列标准合约来使用 Kleros 成为其争议解决机制。此外，我们已提议标准 [43] [61] 来使所有人能来开发无需事前决定何机制将被使用之合约。此标准将使时常参与争议服务的系统用户方能轻松切换不同争议决策提供方案。

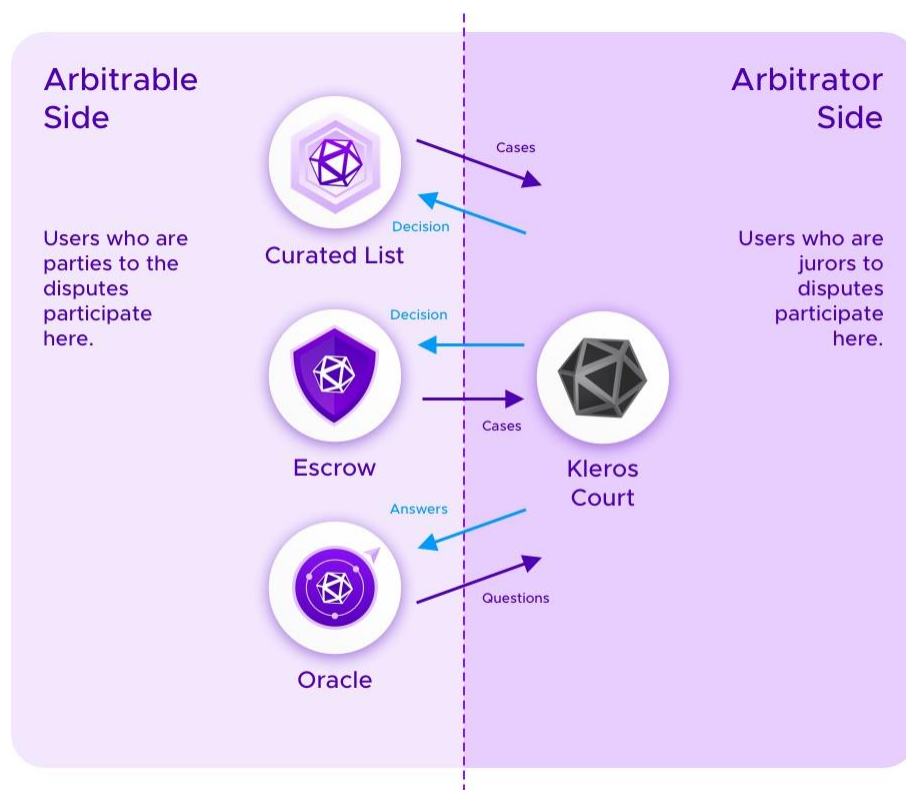


图 3：“可被仲裁”合约，意表可能需要一争议解决方案的合约将被归类于左方。此包含之范例应用方案一为预言机数据提供，代表当用户对于链外真实数据状况有争议；二为策展列表，代表当争议浮现于一用户认为一列表进出案例符合规范认定，但其他用户否决且争议产生；三为及其他一般性第三方托管用途应用，此代表当智能合约持有之价值将依照争议仲裁判断而决定其最终去处。请查看章节 6 来详细了解更多争议应用范例。”可被仲裁”合约指定一“仲裁方”合约如图表右上方的 Kleros 法庭，来提供仲裁决策为所有可能争议。

⁵ 于此论书中我们将论谈关于目前已导入之 Kleros 状态及所有未来可能之提议机制或计画。当我们开始逐步研究开发此类问题，下方提及的可能机制也很有可能于未来做出些许改变。

于不需要仲裁之情况下，合约将足以允许各式各样之可能行为，尤其是于当事人一致同意之情况下。例如，目前 **Kleros** 第三方托管机制包含一有限数量之解决类型系统。

此外，合约将指定陪审员能投票之选项范围。利用先前介绍之范例，此选项可能为：“补偿 Alice”，“给 Bob 额外一星期来完成网站设计工作”，及“支付 Bob”。此智能合约将指定一相对应行动为各可能选项。于此范例：

- “补偿 Alice” 选项将传送资金至 Alice 帐户地址。
- “给 Bob 额外一星期来完成网站设计工作” 选项将给 Bob 整整一星期来专心补偿工作 (Alice 无法于此期间提出新争议)。合约可能被编辑为如选择此选项，其将无法再被提出任何更进一步的争议。
- “支付 Bob” 选项将传送资金至 Bob 帐户地址。

大致上来说，任何有限选项列表都能被提交至陪审员⁶。选项组具有多方不同架构将于某些情况下被调整至少能成为“离散化”程度。其中，我们已研究一机制来使陪审员们能选择一实际数字价值 [31]，来使参与方能获得一比例之退款金。例如，陪审员可能最终决议来退款 75% 回至 Alice 并支付 25% 给 Bob。

4.2 区块链基础架构及扩张方案

Kleros 目前正被导入实施于以太坊区块链，然而，此协议具有能力来被导入于任何智能合约可运作之区块链平台。例如，一 **xDai** 版本之 **Kleros** 正在进行一系列之开发后程序 [50]。请注意，于未来，我们极有可能会见到侧链版本之争议法庭能足以被上诉至以太坊版本之正式 **Kleros** 法庭。确实，一方可能会想要优先安全性当考虑上诉至最强大的法庭版本当面对一攻击或一独特案例；请查看章节 4.8 来寻求更多详细资讯关于上诉机制。

此外，其也有可能来拥有可仲裁方及仲裁方合约介于不同共识机制，简单来说，存在于不同链上的智能合约，例如，一合约可能为于以太坊的乐观卷轴上，而另一合约则是位于另一 **L1** 区块链或另一不同的 **optimistic rollup** (乐观卷轴) 之上 [40]。此将提起可能之沟通问题介于可仲裁方与仲裁方合约间，因虽被部属于同一共识机制上的争议能被及时有效地发起，被部署于不同链或卷轴上的合约仲裁并非运作如此。此相关问题对于 **Kleros** 极为重要为，因其主要被设计来成为一协议来足以互动与需要多方不同类型争议解决的多重 **Dapp** (去中心化应用程式)，而其可能各自被部署至多方不同之开发平台。

沟通机制介于不同链及卷轴将大大有所差异。于一些场合，特别是当可仲裁方及仲裁方合约位于同一乐观卷轴，或一些跨链桥梁的场合，其将存在些许“慢速”的沟通障碍来延迟整体程序晚上几天，并具相对应之挑战期间来使任何第三方能于讯息被传送至另一方前列举 [40] 任何探测

⁶ 陪审员总是能选择一“拒绝仲裁”选项。关于如何激励陪审员，请参照 4.7.3 章节，此拒绝投票选项为永远可行所有陪审员，所以如陪审员具一经济诱因来选择此，如其坚信此选项为最合适之赢家选项。关于一 **Kleros** 普通法庭的政策，换言之，所有现有之法庭的政策，参照 4.3 章节，为陪审员应当选择“拒绝仲裁”选项如此审议结果将被用于部分牵涉非法行动。

之恶意沟通行为。于上述情况下，Kleros 能导入使用图 4 提供之机制来促进被仲裁方及仲裁方的相互沟通，其中用户将宣称关于另一方用户之合约状况。此宣称完全可挑战的，且其具押金保证要求，类似于状态更新交易于乐观卷轴 [40]，然而其被挑战期间将能依照可被仲裁方之应用程序需求来做适当变动，所以一方必须完全等待任何可能争议的“慢速”沟通机制所要求之完整其间。

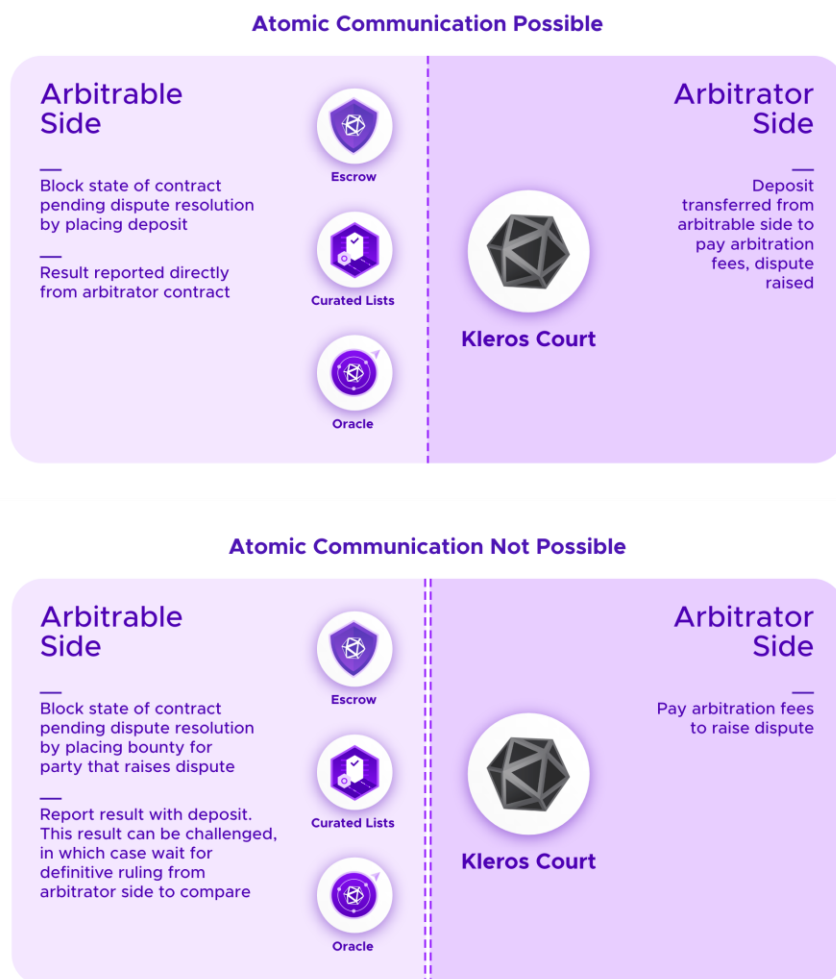


图 4：当原跨链沟通为可发生介于被仲裁及仲裁方合约，一单独交易能同时暂停被仲裁方应用程序并支付仲裁费用来发起一争议于仲裁方应用程序。相似之，争议结果能被立即报告至被仲裁方的应用程序。当原跨链沟通为不可行，但其依然有一“慢旧”沟通方式，例如能来传跨讯息从一乐观卷轴至一 L1，我们能拥有一模式来使一方能汇款比需要仲裁费费用还高额的押金费用来协调仲裁方应用程序的区块状态。而此高额汇款押金将提供成为欲于仲裁方花费仲裁费来提议争议的成为激励赏金。此外，各方将能使用户来与汇款押金同时提交可挑战之讯息至可被仲裁方合约，并使其“于多数情况下”只通常需要花费中等之等待沟通时间，并其只将会进入“慢速”沟通模式如被挑战争议。

请注意，图 4 的非原跨链沟通模式需要额外汇款押金来被完成，而其非一必要场合如被仲裁方及仲裁方原先能直接利用原跨链沟通。尽管如此，一适时关心双方参与链/卷轴的观察者能选择汇款于一几乎无风险之状态。因此，藉由提供一额外费用，系统之流量提供者将能被激励来确实提供服务⁷⁸。

4.3 法庭结构树

当创建一可被仲裁合约，参与方需要为合约选择一指定参与法庭。例如，一软件开发合约将利用一软件开发法庭，而一保险合约将会选择一保险合约等等。

同时，当一方欲登记成为陪审员，此用户需从一般庭开始进入并循从其个人拥有之特定技术才能⁹来发现一合适之专属法庭。各代币持有者将能登记其持有代币至上限一个子法庭于各质押之普通法庭内¹⁰。图 5 解释目前法庭结构树及可行之登记轨迹方案。

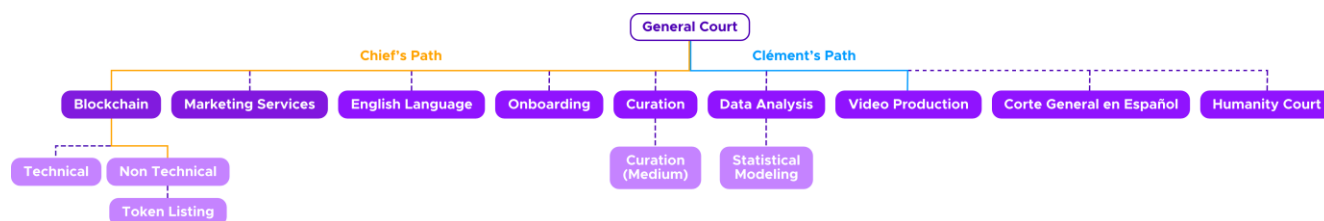


图 5：于目前法庭结构树中，智能合约创建者必须选择其合适之法庭。新类型法庭将陆续被添增至此 **Kleros** 来应对未来可能的新争议需求。此机制来添增新法庭被详细解释于 4.12 章节。而选择陪审员于法庭系统将被呈现于下。Clément 将能被抽选为一陪审员于一般法庭及影片制作法庭。

要求陪审员来自行决定各法庭将激励其来选择最合适之技术才能为最终选项。如其能选择每一法庭，其将有高机率来选择最有可能最大化代币解决争议利益的法庭。

各法庭具有其特定规范及政策。而一部分之参数也将可能被各庭选择利用，其中之包含参数为程序时间，花费成本，抽选陪审员数，及质押代币数。我们将详细介绍此系统于下方之 4.7.3 章节。

⁷ 此外，于些许案例中此结构能被简化。例如，如其中一合约位于以太坊 L1，沟通从其合约至一乐观卷轴将比同样情况之反向操作更加快速。而当争议被建构于无需经济性激励赏金参与来提起争议的模式，例如一方将必然输掉争议如仲裁费不被支付，则其将无法避免来不为可被仲裁方及仲裁方合约来支付仲裁费用。

⁸ 新版本之 **Kleros** 将计画来导入使用以太坊 L2 乐观卷轴。然而，我们也正积极研究 zk-卷轴之相关科技发展，而其将可能被适时导入如 zk-卷轴被广泛利用于一般智能合约。

⁹ 于图解意涵，此结构将以普通法庭为基础来延展数组之子法庭。

¹⁰ 此外，代币持有主必须先质押于母法庭来接着足以质押于子法庭，所以当质押于目前所有法庭的代币持有主将意涵其从之子法庭至母普通法庭的所有路径。

4.4 提起争议

可被争仲裁合约方的性质特性将决定争议将可能于何情况下提议产生¹¹。多数情况下，合约参与双方能提起一争议如有不满任何合约情况，或选择默认同意状况如未有任何争议不满产生。

于任何争议产生情况，合约参与双方能于证据提供期间来提供任何证据来为其代表方来辨明争论。此证据将以符合至 ERC 1497 标准 [61]，而其必须设置标准来为决定证据的组织表列程序及其如何触发智能合约事件，并进一步为仲裁方應用程式提供互通可能性。

4.5 抽选陪审员

4.5.1 质押

用户具有一经济性诱因来成为 Kleros 陪审员并提供审议服务：其主要诱因为收集仲裁工作的奖励费。陪审员候选人将自行选择来服务成为陪审员藉由质押 Kleros-加密-代币，也称为 PNK¹²。而一争议来成功被抽选为陪审员机率将依照陪审员的代币质押数量来所决定。质押代币数量越多，则其可能被抽选为陪审员的机率越高。质押 PNK 于一意涵上意表可能被抽选为陪审员的机率；完全无质押 PNK 的用户将无任何可能性来被抽选为陪审员。此预防非积极的陪审员被系统抽选。

PNK 主要有以下三大主要功能于 Kleros。

- 首先，此保障系统不受女巫攻击 [25]，特别是恶意参与方利用多数创建之克隆帐户地址来为一特定争议提高被抽选为陪审员之可能性。依照陪审员抽选模式，详情请参照 4.5.2 章节，此直接面向的预防措施能，而其代表此类攻击者将必须被要求至少来与其他诚实陪审员候选人具有相同的质押数，详情请参照 4.5.2.1 章节。另一方面，此预防措施将直接源于女巫攻击防治机制，而此安全机制将遵循以上 Kleros 法庭使用的上述模式，详情请参照 4.5.2.2 章节。
- 接着，PNK 提供一激励陪审员们来尽可能诚实地来与其他陪审员们投票一致。换句话说，非与最终多数方投票结果一致的陪审员方将支付部分质押量至与多数判决同调的陪审员方。
- 最终，PNK 将使进行“分叉”来使创建一平行运行版本的 Kleros 可能化，并成为一重要最终机制来抵抗成功实施之 51% 攻击，详情请参照 4.10 章节。

4.5.2 陪审员抽选

一旦候补陪审员已藉由自行选择何法庭来参与并质押于此来表达其愿被抽选意愿，最终陪审员选择将被随机抽选¹³。详细关于如何为此抽选程序生成一随机值，请参照 4.5.3 章节。被抽选为陪审员的机率将与质押代币数有机率关系。

理论上，抽选陪审员基于质押数量将可能使同一陪审员来被抽选复数次为同一特定争议案例。然而，于现实中此为几乎不可能发生如一特定法庭具有一定数量的陪审员及一定程度的多样

¹¹ 例如期间限制，或必须支付给 Kleros 的费用限制，详情请参照 4.6 章节。

¹² 此代币的代表代码 PNK，其命名以 Pinakion 做为参考，而此为雅典公民所使用的一个青铜身分牌匾。Pinakion 时常来成为雅典热门审判中，陪审团抽选的一重要代币象征。

¹³ 请注意，随机抽选已于公共决策实行中被长久地使用。除使用于陪审员抽选外，此机制也被用于选择公共官方领导人于古代雅典及维也纳再生期 [22]。详细关于此抽选程序的公正性，请参照 [26] 及 [58]

化质押池。尽管如此，我们将依旧来按照女巫攻击预防措施如何被达成，及其同一地址能否为一特定争议来被抽选复数次等特性来提出两抽选陪审员的主要模式。

何模式来被子法庭所采用将依据一参数所决定，而其将能够被治理程序所作调整，详情请参照 4.12。

4.5.2.1 藉由代币达成女巫攻击防范

值得注意的是，于 4.5.2.2 章节解释之女巫防范可能方案限制每一地址能投票的次数，但其将使恶意行为者来将质押代币数量平分至多组地址来欺压诚实参与者。来减低此操纵发生机会，根据此模式，机率来抽选同一候选人两次(或多次)为允许的。用户被抽选之次数来为一争议(称为权重)将决定投票数权及可能于此争议中获得或损失之代币额。因此，相较于持有代币于同一地址，一攻击者将无法获得额外利益来藉由平分其代币至多重帐户地址。总结来说，如攻击者欲具有高于半数之投票权于此规则模式，其必须至少拥有超过质押数总量的半数以上，关于 51%攻击更多详情，请详细参照 4.11.1 章节。



图 6：想像 6 名代币持有者质押总计 10,000 代币于以上情节。而其中 5 枚代币被选取，编码 2519，4953，2264，3342，及 9531 代币。因此，代币持有者 B，C，及 F 被抽选为权量 1。而代币持有主被抽选为权量 2。

查看图 6 来查看一陪审员抽选范例。请注意，质押之 PNK (除了被与多数决不符的陪审员所质押的)将被于最终审议完成后归还原主。

4.5.2.2 藉由人性证明达成女巫攻击防范

于未来版本的 **Kleros**，一额外女巫攻击预防措施将得以使用。于此，来足以被选成为陪审员于此法庭模式，其陪审员之帐户地址必须已先注册于人性证明 [38]，一防范女巫攻击的人类注册列表，详细请查看图七。其由使用 **Kleros** 法庭之机制来策展列表，特别是用于”人性法庭”及其上诉法庭(们)，来决策审议申请之案例是否为克隆或带有恶意之帐户。

用户复杂性可能随此登记机制导入而有所增加，不过此模式机制将使一帐户地址只能被限制于最多一票而其能顺带消除任何恶意行为者来利用平分代币至多重帐户地址来欺压诚实参与者用户的可能性。

此模式机制于 4.5.2.1 章节为部分有用对于任何仲裁解决任何关于人性证明的相关争议的法庭，例如人性法庭及其上诉法庭(们)，特别为一般庭。确实，使用人性证明来自行提供女巫攻击预防为牵涉到自己本体机制的法庭将导致多重额外安全疑虑保证且限制人性证明之有效性，并让使用其女巫攻击防范扩张机能之法庭来从难以从攻击快速回复。此外，此模式机制也将自然发展为一充满达到资格的质押陪审员法庭，但只有少数注册于人性证明能来参审。

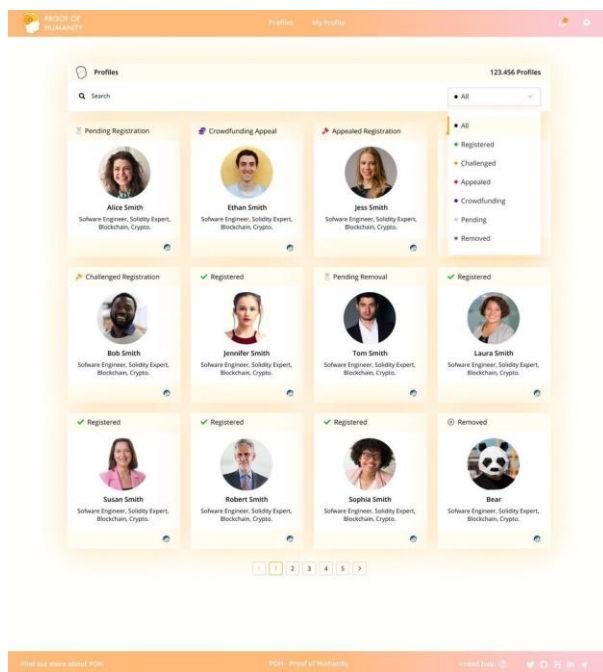


图 7：人性证明为一真实人类的精选列表清单，而如关于其列表之提交帐户是否确实为克隆或假造的身分之争议发生，其将被仲裁藉由 **Kleros**。于未来 **Kleros** 版本，特定法庭将可能采用人性证明，而其将表示如任何人欲成为此法庭陪审员，其必须先登记于人性证明，此人性证明列表将间接性帮助预防恶意行为来使用多重假造或克隆帐户来操纵审议。

4.5.3 随机数值生成

来抽选陪审员，一不受操控的随机数值生成机制为必要条件。使用一协议来创建一随机数值于参与者双方 [8] 并非可行。一攻击者能与自己本身来创建提起一争议，选择自己来成为陪审员多数次，并选择另一受害者陪审员来参与。而其将接着故意与受害者陪审员投票相异并同调协调其控制之投票权来使其符合多数决，且最终从受害者陪审员方偷窃重新分配之 **PNK**，详细关于此激励机制系统，请参照 4.7.3 章节。

4.5.3.1 随机数值生成利用区块哈希

目前，随机数值来抽选陪审员为源于以太坊区块哈希。虽此数值为几乎无法来事前预测，矿工可能来决定来不适时释放一区块，而其可能将使随机数值变得不有效，但此场合也代表矿工必须丧失挖块之可能区块获利。

4.5.3.2 随机数值生成利用阈值签名

另一可能的随机数值生成机制为利用一阈值签名为基础。此概念为利用一“**钥键 - 持有者**”来生成 n 量中 f 数的阈值签名，并利用一应对之公钥来互动。例如，一方能使用一阈值版本之 [10] **BLS** 签名架构 [11]。接着，为了来生成一随机价值，一方提供之随机种子将被初始化，而其能被公钥作来验证其为正确无误。而只要阈值签名中 t 钥键 - 持有主足以参与，此结果之签名将成为一固定价值数，而其将不受任何 $n - 1$ 数量之钥键 - 持有主的动作所影响。换言之，无一小于 $n - t + 1$ 的团体将能更改此随机价值数，或来避免此机制来生成一随机值。此外，无一小于 t 之勾结团队将能足以来提前获得回覆一随机值。请参照 [24] 来了解此方向之相关研究工作；特别是使用此方案的 **Chainlink Verifiable Random Function (VRF/ Chainlink 可验证随机函数)** [23]。

4.5.3.3 随机数值生成利用顺序性工作证明

另一未来可能方案为使用一验证延迟函数功能 [9]。一方式来生成此函数功能是利用工作量证明为基础，例如，利用相似于 **Bunz et al** [20] 提案的架构。此架构概念主要为一最低限度的时间，基于一最快速的硬体设备来进行一特定非平行可行的计算程序，应该为一需求特性来计算生成随机值。接着无一方能来预测生成之随机数值快速于此计算下限。

我们稍微解释此架构如下：

1. 初始化：刚开始为随机种子=区块哈希，而使所有参与方能输入一价值当地随机值来更改随机种子来使随机种词=哈希(随机种子，当地随机)。此将被所有参与方允许来更改此随机种子。此也为一关键来使随机种子不被任何一单一参与者来自行选择。使用以上程序，所有参与方能变更随机种子，但无法选择此，因为选择一特定之随机种子攻击将必须使攻击者来决定当地随机值并使哈希(随机种子，当地随机)=随机种子攻击，而其将极为困难达成基于密码哈希函数的原向抗性¹⁴。

¹⁴ 请注意，于此列表之协议将适应工作量证明及权益质押证明的区块链。于工作量证明区块链，区块哈希几乎为无法事前来被预测，而一方能移除初始步骤来只使用区块哈希来作为随机种子。然而，以太坊正目前计画来转换至权益证明。

2. 计算最终随机数值：有牵涉随机数值生成的各方参与者将运行一顺序性工作证明于随机种子。从 $h_0 = seed$ 开始，其将计算 $h_{n+1} = hash(h_n)$ 来使 h_d 成为 d 困难度参数。计算 h_d 将花费些许时间并保证其将有时间间隔于取得随机种子知识及取得结果。此困难度 d 将被固定为使无一硬体能够来计算 h_d 界于初始化阶段。因为无一参与方需要前一步骤之结果来开始此新一步骤，其也代表此程序将无法被同时平行运作。而这也意涵着无一单独参与方能够来比其他参与方来更快速的获得结果。

3. 取得结果于区块链：各方参与者皆能公布 h_d 利用一发现汇款押金。其他参与者接着能尝试利用互动性验证 [51] 来证明此结果为是否正确的。此包括对于攻击者结果进行二分搜索。如一攻击者提交一错误 h_d ，一诚实参与方将能寻问其关于 $h_{\frac{d}{2}}$ 的价值。而如回答方提供一错误价值回覆，其代表攻击者价值介于 h_0 至 $h_{\frac{d}{2}}$ 有错误出现。如其回覆正确价值，其代表 $h_{\frac{d}{2}}$ 至 h_d 有错误产生。不管何方式，检索范围将为全体之二分之一。而诚实参与方将持续来减低此搜索范围(无论错误为何处)来使最终只剩下两价值。接着诚实参与方能展示 x 来表示 h_{x+1} 不等于哈希 (h_x) 于攻击者解答，并使其回答无效。无效回答之参与者将损失其汇款押金。请注意，此互动数值来与一非有效错误结果只需要 $O(\log(d))$ 。

4. 获得所有随机价值：所有诚实参与者验证结果后，其将只有剩一正确结果 h_d 。从此最终随机价值我们将能利用如 $r_n = hash(h_d, n)$ 函数来生成许多随机价值。

如至少一诚实参与者于系统内，以上此程序的输出结果将为一随机数字。计算此顺序性估作量证明及激励验证需要些许时间。但为多数从争议产生至陪审员抽选间只会花数小时等待之争议，其将不会成为任何问题。然而，为一些特定争议需要短处理时间(例如，一法庭处理去中心化社交平台的内容监管争议)，此随机数值生成程序可能将为太过慢速。

使用之随机数值生成技术将有所变更依据目前何可能方式为使用于当下使用区块链上，详情请查看 4.2 章节。例如，非当地原生符合乐观卷轴平台之区块链 [40] 将不会适合此随机数值生成方式。于另一方面，阈值签名架构之机制如 Chainlink VRF [23] 为设计为此类型平台。验证延迟函数，如先前介绍之顺序性工作性证明架构，可能足以提供一长期上诉方案。

4.6 仲裁费用

Kleros 使用仲裁费用来奖励陪审员的工作贡献。此费也用来使其将更加困难地来创建假帐户来对系统进行讯息滥发攻击。与最终多数决结果同决议之各陪审员将被支付奖励，而其额量将依照争议解决之法庭来做决定。可被仲裁方智能合约将最终决定何方参与者将支付此陪审员费用，而此将依据各场合有所变化。

此规则其实很简单。例如，其可能将要求创建争议之参与者来为此争议费做支付。然而，我们也能考虑更加复杂之设计来创建更佳良好的激励特性。例如，一方将能要求合约各参与方来汇款一相同额量之陪审员费用至一智能合约内。如单一参与方无法完成此，合约将自动宣告汇款

仲裁费方为默认胜利方(而无须创建一争议于法庭内)。如双方确实汇款此仲裁费，则胜利方的汇款押金额量将于争议结束后被补偿。

4.7 投票及诱因

4.7.1 投票程序

陪审员入手被提交之证据(通常被提起争议方所提交)，了解各法庭政策，比较与陪审员指示¹⁵，并决定关于其如何论理争议基于此提供证据。

接着各陪审员将提交 [13] 投票来决定其意见决策对于此争议案例。换言之，其提交一哈希(投票，随值，地址)¹⁶。于未来版本之 **Kleros**，陪审员将能够利用与一新随值来重新提交一决策承诺于投票期间，来重新确认一既存投票或来挑战一投票。当投票程序结束，陪审员将揭示{投票，随值}，而 **Kleros** 智能合约将验证此确实符合(最终)接受之投票提交。陪审员失败来揭示其投票，其将会被惩处，详情请查看 4.7.3 章节。更多详情关于此程序来提交一投票利用一哈希价值，特别于投票期间内限制其他陪审员的资讯息可视性，请参照 4.9 章节。

4.7.2 投票聚合

于各轮投票期间最终期，投票将由各陪审员揭示。无揭示其投票之陪审员将被惩处。最终，投票将被聚合依照先前决定之投票规范，而其将最终使一案例赢家产生。

4.7.2.1 目前投票系统

当陪审员被提供一二元选项，此为自然来使用”多数制”投票系统¹⁷。目前，**Kleros** 也使用多数决性统为其他非选项争议案例。(具体来说，赢家选项为多数制投选项于最终投票揭示轮，详情请参照 4.8 章节)。

多数决机制可能产生以下情况于一多于二元选项之投票状况：

- 许多可能之诚实选项(或”克隆相似选项”)。而其将诚实投票之陪审员票数分割，并减低其最终赢出的机率。举例来说，想像以上提及之 **Bob** 范例与多重选项，**Bob** 获得另一周工作期间，另一八天工作期间，或另一九天工作期间，其各自为单独选项。而其类选项之总和投票数将被集成一大范围选项来表示”给 **Bob** 额外时间”的选项，详细请参照图 8。
- 其可能演化至无一选项能获得高于 50%投票数之情况场合，而此将减低系统防御针对攻击所需要的可能票数门槛来使不诚实选项最终赢出，详情请参照图 9。

¹⁵ 此政策将依法庭而有所异，详细请查看 4.3 章节，而关于创由治理程序的政策变更，请参照 4.12 章节。

¹⁶ 而此论文内我们使用哈希来意表加密哈希功能函数，于以太坊，其为 **kec-cak256**。

¹⁷ 多数制，或多数决，为一投票系统来使投票参与者能为单一候选人表明投票意向，接着获得最多投票数之候选人将被最终选择，即便其可能没达成过半数投票，其依然会成为系统最终选择的选项。

考虑到以上种种问题因素，一方可能预测多数制投票将生成大致”诚实”结果如诚实选项为十分清楚明了，而其类选项自体本身也通常已二元化其选项。然而，Kleros 也正目前朝向多选项可能案例进行积极开发。

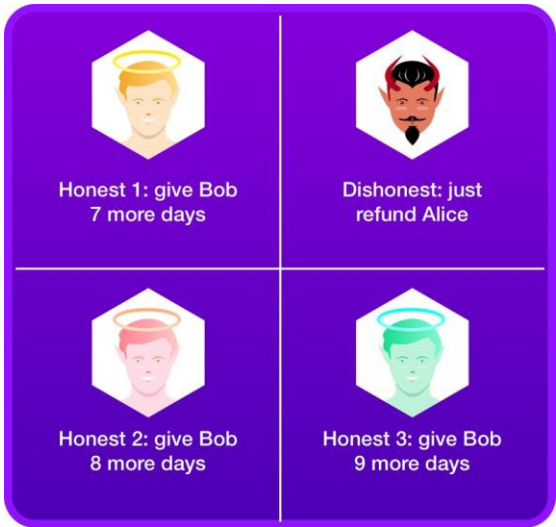


图 8：于此多数制投票系统，陪审员只能投票选择单一选项。特别是，如一投票者无法投票支持一选项类似”选择一个最花时间的选项，我不管”。而如果陪审员被提供一系列之诚实选项及只有一个的非诚实的选项组，此独特单一的非诚实选项组将可能意外成为系统谢林点。

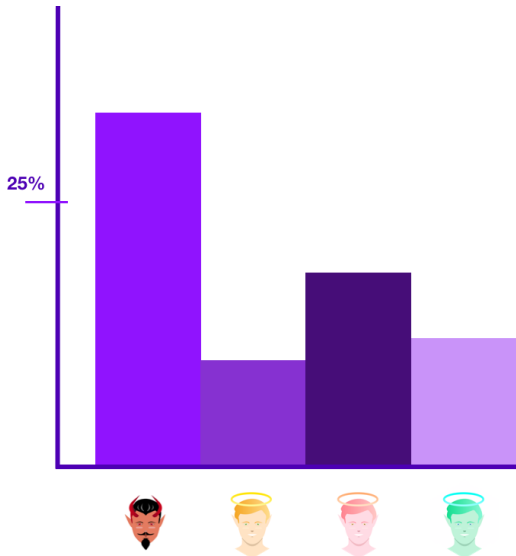


图 9：如投票被多组”诚实”选项分割，一攻击者将可能不需要来贪腐 50% 以上的投票于多数制系统来使恶意选项被采选。

4.7.2.2 社交选项及未来投票系统(们)

于此章节，我们将考虑一系列形容特性于一投票聚合裁决系统如 **Kleros**，来了解何裁决符合及不符合此些特性。此类投票聚合裁决假设陪审员应当为争议案例提交客观的细节资讯，而非自行认为最合适的简单结果呈述；此投票时常成为阶级排列结果型式 $a_1 \geq a_2 \geq a_3 \dots \geq a_n$ 。于章节 4.7.3，我们将讨论可能的支偿架构来激励参与者于此系统内。请注意，为一些考虑之特性，一分析关于一投票结果聚合将依据选择之激励架构变化而有所影响。确实，当我们清楚分析讨论投票结果聚合及支偿架构，此选项为时常为息息相关，各有其优缺点，且必须常常被一起来考虑。此外，虽然些许被考虑之特性确实具有高标准定义，其他些许特性也有可能不时为模糊客观。

于未来版本 **Kleros**，建立法庭的智能合约架构将更具组块性。特别是，此将可能来使智能合约能被编辑利用相异之投票及激励机制，且同时能被执行由一现行法庭合约。关于何投票及激励机制被允许利用将由协议之治理机制所决议，请参照 4.12 章节。为不同应用程式，其为合理来均衡选择及优化其需要之可能特性。

理想情况下，一投票聚合机制系统应具有以下特性：

- 克隆抵抗 – 从一投票系统的观点来看，此为一重要标准特性来被考虑于社群选择理论，而其也多少意味着拥有一“克隆组”的多相同选项将于一定程度下，非直接增加或减少克隆组以外之选项的获赢率，更多详细关于此正式定义解释，请参照范例 [60]。使用一克隆抵抗的聚合裁决系统将使参与者能生成随意合约且无须来担忧此给予至陪审员之两或多代表选项将导致投票量分权或与原先意见分歧。

一克隆抵制之投票系统之范例为 **Instant-Runoff (IRV/立即经流)** 系统，**Ranked Pairs** (阶级排列配对组)，及 **Schulze**(舒尔茨)。此结果将呈现于以下图表之克隆抵制区栏，以一投票系统标准型式，就如呈现于 [60] 及 [56]。值得注意的是，如于一假设情况，一更加强大的克隆抵抗概念可能不仅要求投票来独利抵制与克隆行为，其能更进一步地使任何预期之克隆行为将不会影响到任何投票者将接收之预计支偿，或至少不会影响何投票将护得最佳酬报支偿，而其包含对于克隆组内的其他可能选项的选项排列。

尽管如此，我们已启发式/数字式地来详细分析此类系统，而我们注意到 **IRV**-类型系统，虽确实为一克隆抵制投票系统，拥有一偏见倾向于克隆奖励对于 4.7.3 章节所考虑到的支偿系统。确实，如一投票者将一克隆组考虑来作为最高优先层级于一克隆的 **IRV** 机制系统，首先高阶克隆投票者的克隆系统，其将比低阶层之克隆阶层起具有更多的影响力。因此，基于投票者最终排列赢家之比较来奖励或惩处投票者的激励系统将使投票者来阶级排列一克隆组至高阶来获得一稍微高比例之奖励于克隆组添增选项后。我们，至少启发式的分析中，还未发现此偏见倾向于 **Ranked Pairs** (阶级排列配对组) 或 **Schulze**(舒尔茨) 系统内，而于其类型种类系统，聚合裁决将基于相对强度的配对对抗。

- 满足 **Condorcet** (孔多塞) 标准 – 一投票裁决时常被称为一孔多塞方案，其代表如一 w 选项存在，而阶级 w 的投票者具有多数相较于 a 和所有 a 以外之选项，则 w 将胜出，更多详情请参照 [12]。请注意，此“孔多塞赢家”并非存在于所有陪审员所表

意之投票决定中。如果一选项相连赢过其他选项而此选项将被选择，则其想法可能为太过于直觉性。因此，如果 Kleros 案例时常拥有孔多塞赢家，则其意表其对于陪审员为比较直接容易的理性开想。此外，孔多塞标准，特别是偏好选项具有一共识来对抗其他选项的群体，将应对至一定程度概念之“平等性”。

另外，我们能见到孔多塞特性，如协调与先前于 4.7.3.2 章节讨论之激励系统结合，也将具有一积极效应于攻击预防性。确实，一攻击尝试(失败)来驱逐一孔多塞赢家藉由逆转捕捉之结果及欲使用之可能方案，将导致激励机制系统的惩处结果。Ranked Pairs (阶级排列配对组)和 Schulze(舒尔茨)为孔多塞方案的其中方案。

WoodSIRV 为一孔多塞-化之 IRV 版本来检测各投票轮藉由检视其是否有合适之孔多塞赢家，并将自动选择此选项如其为确实存在。

- 攻击抵抗性 – 请注意，攻击抵抗性为基本上意涵与一经济性质。例如，一方可能会想来更改投票数量来使“非诚实”选项最终拥有高机率来赢出，与一理由表明其可能使攻击成本增加，例如来变更投票所需要之贿赂。因此，攻击预防主要包含被社交选择理论所研究过的特定标准投票系统特性，例如 Later No Help(稍后无害)及参与标准 [12]，与一结合利用奖惩分析于激励系统，详情请参照 4.7.3 章节。

当一方能实施攻击于单独系统，此为非常困难来生成证据来表明无攻击存在¹⁸。讨论于 4.7.2.1 章节已显示如一 51%攻击将拥有一较低攻击门槛于多数制系统如无单一(诚实)选项接收多于 50%之投票权。于 Borda(博达)系统，如此“诚实”解答为 a 且攻击者希望选项 b 来赢出，其能提交多数投票来使 a 被阶级排列于首而 b 为次，且少部分投票来使 b 为首且 a 为最后。使用形容于 4.7.3 章节之激励系统(们)，此攻击将为攻击者减低攻击成本及风险，而同时适当选择参数，Instant-Runoff (立即径流) 及 Ranked Pairs (阶级排列配对组)似乎对此攻击较具预防性¹⁹。

此也值得注意的是，考虑于 4.7.3.2 章节之操纵激励系统行为为可探测及可惩处的，所以请尽量避免选择一激励系统并非惩处之易操纵聚合功能函数。我们已于先前提到，当一攻击来预防一可能之孔多塞赢家来胜出为极容易来探测利用我们考虑之激励系统。于另一方面，根据 Arrow 的 Impossibility Theorem (不可能性定理) [5]，对于所有非平凡的投票系统，其将可能有一“无关连可能”选项阶级排列而影响最终结果的场合。操纵包含此无关连可能将不会被我们于 4.7.3 章节²⁰所考虑到的激励系统所讨论。然而，请注意，Instant-Runoff (立即径流)满足 Later No

¹⁸ 因此问题宣称将更佳攻击预防于 Instant-Runoff (立即径流)，WoodSIRV，Ranked Pairs (排列配对组)，及 Schulze(舒尔茨)将于以下图表。

¹⁹ 所有我们的宣称于攻击预防将被视为基础于激励机制系统于 4.7.3 章节。此为可能来利用另一激励机制，而我们的结论也将因此而可能会有所不同。也请注意 β 的扮演脚色被讨论于 4.7.3 章节；为使 $\beta = 0$ 权重于系统 2 及 3，经济成本于损失提款金于攻击形容于 Borda(博达)为可比较至一攻击于 Instant-Runoff (立即径流)，当攻击者能贿赂许多投票者来使 b 被阶级排列首且 a 次，而利用一攻击于 Instant-Runoff (立即径流) 需要来说服一多量陪审员来接受可能之小额惩处，及攻击于 Borda(博达)需要说服少量陪审员来接受可能之巨额惩处。然而，与其他 β 选项，此攻击于 Instant-Runoff (立即径流) 为更加昂贵，而攻击于 Borda(博达)为较非昂贵。

²⁰ 此为一系统顺序拥有赢家优先，最大限度支偿特性形容于 4.7.3 章节。因此，此激励系统无法来辨别比“非相关代替”选项还低阶级排列之重新排列支偿。

Harm(稍后无害)及 Later No Help(稍后无救), 而此操纵将只会有关连至一定程度来影响比其他代替方案还可能优先胜出之先前已存在的高阶级排列选项。因此, 于此系统, 一方能来将预测来使生成一非诚实选项, 一攻击者必须先尽可能贪腐所有先前欲投票至”诚实”选项之投票者。

因此, 我们争论投票系统如 WoodSIRV, 为孔多塞机制但解决孔多塞悖论利用 IRV 相似步骤, 而其看似提供一更佳方案来对于攻击预防性因其结合此不同层别之防御, 并要求攻击者需要来承受所有可能成本来预防可能的孔多塞-赢家, 并使其之一赢家足以被操纵的程度来发现自体本身于一孔多塞悖论, 并自觉只有藉由操作已接收巨额惩处之投票者将有效, 且限制有效攻击至 51% 攻击需要的启发式同盟²¹。

- 无需太过要求程式复杂性及 Gas 费 – 即使于一扩张版本之以太坊, Gas 花费将还是极有可能持续成为一忧虑。此外, 于任何智能合约平台, 减低程式复杂型为非常有效对于减低程式漏洞瑕疵。为所有考虑之投票系统, 赢家将被能被计算出于一项式时间。然而, 对于投票系统使用一 IRV-类型, 整数基础架构将可能比起需要图解演算法的 Ranked Pairs (阶级排列配对组)和 Schulze(舒尔茨)还易导入。
- 预防来拥有太多”谢林-非诚实场合”/单调 – 我们已见识到工作成果于[30], 位任何激励系统, 其将必定有些许稀有场合来使投票者来无意或刻意地远离开从熟称之”谢林-诚实性”, 简单来说, 其将被激励来投向一其本身其实认为不会赢的选项。先前研究建立于经典机率理论于社交选择论如 Arrow’s Impossibility Theorem (不可能

²¹ 我们先前已尝试来解释针对 WoodSIRV 和 Ranked Pairs(排列配对组) 攻击的差异, 并利用些许范例。因两系统同为孔多塞, 如其有一”诚实可能”选项 w , 于两范例中来欲变更最终结果, 攻击者必须先操纵足够投票者来预留足够票数与 w 相对应。如预留此结果于一新被选择之孔多塞赢家, 此相同操纵行为将拥有相同结果于两系统。当然其也可能具有其他投票可能性来使一或多投票系统必须要求更多操纵于投票者来足以变更最终结果。此一状况范例为当更多投票被要求来变更此结果于 Ranked Pairs (排列配对组), 考虑到 2 票为 $\{a>b>c\}$, 5 票为 $\{a>w>b\}$, 8 票为 $\{b>w>a\}$, 及 6 票为 $\{a>b>w\}$ 。此 w 为孔多塞赢家, 但因已有一操纵正尝试变更 $\{a>w>b\}$ 票至 $\{>>\}$ 并导致一情况为 w 其实获得最少首位阶级选项票且被剔除于 WoodSIRV 系统的孔多塞悖论。来变更结果于 Ranked Pairs (排列配对组), 攻击者能尝试以下工及策略 1) 其能尝试贿赂来使其他投票者变更投票选项, 例如从 $\{a>w>b\}$ 至 $\{a>b>w\}$ 来增强 $b>w$, 2) 其能尝试来变更投票从 $\{a>w>b\}$ 至 $\{a>b>w\}$ 来减弱 $w>a$, 3) 其能尝试来贿赂说服更多投票者来变更, 例如, 从 $\{w>a>b\}$ 至 $\{w>b>a\}$ 来减弱 $a>b$ 选项, 4) 综合策略。变更于前两策略, 于某程度上, 如不直接成功更改 w 结果, 将导致其投票落选, 而投票者遵循第三策略并投 $\{w>b>a\}$ 将依然获得最大化支偿如 w 持续为赢家。于此, 此可能为更加方便来让一攻击者来贿赂说服投票者本来就愿投票 $\{w>a>b\}$ 至”微-作弊”的 $\{w>b>a\}$ 选项相较于其他可能操纵可能性。另一方, 考虑到投票显示 5 票为 $\{a>b>w\}$, 2 票为 $\{a>w>b\}$, 5 票为 $\{b>w>a\}$, 7 票为 $\{w>a>b\}$, 及 2 票为 $\{w>b>a\}$ 。接着一攻击者能变更及果于 Ranked Pairs (排列配对组) 从投票选 w 为一孔多塞赢家至选择 b 于一孔多塞悖论藉由说服 $\{w>a>b\}$ 票数为 $\{b>w>a\}$ 选项投票。于此案例, WoodSIRV 将依然选择 w 为赢家。确实, 一欲变更结果于 WoodSIRV 的攻击者将拥有多方可能策略 1) 贿赂说服投票者来逆转 a 和 b 的阶级排列来使 b 成为孔多塞赢家, 2) 贿赂说服些许将 a 置于第一阶级排列的投票来放置使 w 或 b 成为首阶级排列, 以使 a 能被剔除于 IRV 程序, 并使 b 于与 w 的相对恒抗中最终赢出。例如, 攻击者可能贿赂一额外投票者来变更其投票从 $\{a>b>c\}$ 至 $\{b>a>w\}$ 。此两攻击策略可能牵涉到换位非权重选项如 w 最终赢出。如攻击者能成功遵循第一策略, 其能变更结果于多孔塞系统。然而, 遵照第二策略, 其将不是要求换位配对需要牵涉与 w , 所以需要被惩处如 w 最终赢出, 就是换位配对至一先前已被列为 w 以上阶级排列的另一可能方案。因此, 此将限制攻击者的能力来贪腐投票来只能换位已决定不想投至(”诚实选项”) w 的投票者, 而此场合将也能被考量为无论如何都将成为共谋攻击。

性定理) [5]，及 Gibbard Satterthwaite Theorem (吉巴德·萨特思韦特定理) [32] [54]。然而，此研究成果见证于此投票机制失败来达成谢林-诚实性场合为似乎更加人为且感觉更不容易来发生于多数特定的投票机制及激励系统。值得注意的是，当一投票系统为较单调设计的，此类型谢林-诚实性失败的发生场合将被大幅减少。

以下图表总结如何选择投票系统基于提供之各项标准：

	Clone Independent	Complexity/ Gas	Condorcet	Monotonic	Attack Resistance
Plurality	No	Low	No	Yes	Bad
Borda	No	Low	No	Yes	Not great
Instant-Runoff	Yes as voting system Bias in incentive system	Medium	No	No	Better?
WoodSIRV	Yes as voting system Bias in incentive system	Medium+	Yes	No	Better+?
Ranked Pairs	Yes as voting system No known bias in incentives	High	Yes	Yes	Better?
Schulze	Yes as voting system No known bias in incentives	High	Yes	Yes	Better?

当陪审员被提供一二元选项，而其也刚好是最常见之应用场合于 Kleros²²，此投票系统为相对的。而确实，投票介于两选项将满足所有”良好”特性于此图表。因此，此图表比较将只会呈现相互关系性于当至少有三可能结果被考虑之场合。

最终，请注意的是当 Kleros 的设计选项为被激励由攻击于一无信任之权威体之一特定挑战场合，此被先前考虑特性则将可能会来相关联远至区块链應用程式，至涉及所有其他众筹意见平台，如 Amazon 的 Mechanical Turk [1]系统，其需要一聚合用户意见回馈来使欲推动讯息滥发攻击或错误讯息攻击的用户需要至少花费一最低的系统成本。因此，此些许想法主意可能将被改进设计此类似系统利用[46]之思想精神。

4.7.3 激励系统(们)

用户能被激励来成为 Kleros 陪审员并使其一机会来可能获得一部分争议事件所支偿的仲裁费，详情请参照 4.6 章节。激励系统将激励陪审员来选择提供诚实裁决选择并获得仲裁费，陪审员可能

²² 其实，所有 Kleros 处理之争议也将有一”拒绝仲裁”的可能选项，详情请参照 4.1 章节。然而，其将被预测此选项将不经常来被选取，所以只拥有两可能选项的案例将通常成为实际二元选项因其只拥有此两可能选项来被投票。

会损失些许 PNK 质押量如其裁决与多数其他陪审员相异。此损失 PNK 额量将被重新分配至其他更加与最终裁决结果同调的陪审员，而其详细程序将被解释如下。而陪审员将参与于一谢林游戏，类似形容于 2 章节所提及的范例。

来使成功被抽选为一陪审员于任何法庭，用户必须来质押一最低限度的法庭质押量，其将被表示为最低_质押。接着，无论陪审员以何方式来投票于一案例，与多数不同调的失败投票将可能损失之 PNK 数量将被限制至此最低限度质押量的一部分比例。此比例将被表称为 α 。然而，于先前 4.5.2 章节的”权量”讨论，一单一陪审员可能会被抽选多次为同一案例，来使其具有多数投票次数于同一案例。则此陪审员的最大限度失败损失量将与其增加的投票数成正比。换言之，最大可能损失的代币额量为—陪审员为：

$$D = \alpha \cdot \text{min_stake} \cdot \text{weight}.$$

其中 α 和最低_质押参数由治理机制所决定且能于各法庭有所变化。

4.7.3.1 目前代币分配模式

目前，与形容于 4.7.2.1 章节的多数制投票系统 (特定陪审员并不提供选项阶级排列除了唯一选项) 平行发展，任何陪审员不选择最终赢出结果 w 于最后上诉轮将会损失其汇款押金 D 。接着投票至选项 w 的陪审员将获得一支偿：

$$\frac{\text{ETH fees and lost deposits}}{\# \text{ jurors that vote for } w}.$$

此结果额量(换句话说，多少汇款押金损失及多少陪审员投票为 w)为计算于各轮审议。

4.7.3.2 未来代币分配模式

来使 w 成为赢出选项藉由投票聚合机制形容于 4.7.2 章节。我们讨论关于陪审员是否”同调”投票如其同意最终投票结果；当成为同调为一零或全的特性为一组二元选项，而为一组非二元选项，陪审员的投票将能来成为大致”同调”。此目标为来激励用户来选择其相信的”诚实”选项结果，遵循讨论于 4.7.2 章节的动机排列顺序。相反之，参与者可能会想要来强烈惩处将赢出选项 w 阶级排列至最下方的陪审员。一方式来达成此为使此陪审员损失：

$$\frac{\# \text{ options ranked above (or equal to) } w}{\# \text{ total options} - 1} D \quad (1)$$

来使其被重新分配至其他陪审员基于同调程度状况。然而，于此建立架构下，一攻击者来使恶意选项阶级排列第一并使 w 排列第二将只会冒着小部分汇款押金的风险。

于方程 1，陪审员将被奖励其以相同权重来正确将 a_i 选项阶级排列至赢家 w 选项下方的选项 a_i 总和数量。另外，其也能选择来赋予额外权重至选项 a_i 的奖励及惩处，而其对票差额量介于 w 和 a_i 可能极为接近。基于此精神概念上，狭隘失败攻击通常应为非常昂贵，而此为一重要目标当设计一区块链-基础平台 [17]。如一攻击者尝试来进行一贿赂攻击，并使一孔多塞赢家选项 w^* 不再赢出，此将需要来准备足够的贿赂数量来使些许 a_i 能击败 w^* 。因此，至少一组配对符合必须使赢家选项不胜出，所以于狭隘攻击此选项配对将被赋予更多权重。

换言之，其可能将使权重 $w(i) = w(a_i) \in [0,1]$ 为所有 $a_i \neq w$ ，例如 $\sum_{a_i \neq w} w(i) = 1$ 。接着，一投票者 USR 将损失：

$$D \sum_{a_j \neq w} \mathbf{1}_{USR \text{ voted } a_j \geq w} \cdot w(j)$$

从其汇款押金 D 并获得重新分发从：

$$\frac{\text{ETH fees and lost deposits}}{\sum_{USR_k \in V} \sum_{a_j \neq w} \mathbf{1}_{USR_k \text{ voted } a_j < w} \cdot w(j)} \sum_{a_j \neq w} \mathbf{1}_{USR \text{ voted } a_j < w} \cdot w(j), \quad (2)$$

而 V 为投票者组于一与 USR 相同的投票轮。而于以下内容，我们将凝聚标记符利用 $USR_k: a < b$ 来表示投票者 USR_k 将选项 a 阶级排列于选项 b 的下方。

请注意，于拥有 M 投票者的场合，此奖励及惩处生成一支偿为 USR 于

$$\begin{aligned} & \frac{\text{ETH fees} + \sum_k D \sum_{a_j \neq w} \mathbf{1}_{USR_k: a_j \geq w} w(j)}{\sum_k \sum_{a_j \neq w} \mathbf{1}_{USR_k: a_j < w} w(j)} \sum_{a_j \neq w} \mathbf{1}_{USR: a_j < w} w(j) - D \sum_{a_j \neq w} \mathbf{1}_{USR: a_j \geq w} w(j) \\ &= \frac{\text{ETH fees} + MD}{\sum_k \sum_{a_j \neq w} \mathbf{1}_{USR_k: a_j < w} w(j)} \sum_{a_j \neq w} \mathbf{1}_{USR: a_j < w} w(j) - D, \end{aligned}$$

利用上一表达方程来避免多余计算步骤。

于此支偿机制下，无论何权重函数 $w(i)$ 被选择，如陪审员将赢出的选项阶级排列越低，则其将会获得越少仲裁费用。确实，如一陪审员将最终赢出选项阶级排列置最后，其将接收零仲裁

费并损失其全额之汇款押金，而其损失额量将被平分于其他将选项 w^{23} 。以上方程为并非涵盖一被零所分除的可能性除非所有陪审员同时投票至同一赢出选项并弃置其他(非零权重)可能选项于一审议轮中，而如此情况发生，所有投票者将损失其汇款押金并无法获得支偿²⁴。

而为选择之权重函数，一系列之取舍及批评关于此将被呈现，相似于 4.7.2.2 的投票系统章节。而我们将把此论坛分隔为两主要讨论区域，一为投票系统，而另一为激励系统，此两选项能于些许场合双互通并应该适时的被一起讨论。

来呈现权重函数选择的各项取舍，我们将提供些许考虑之权重函数。于所有场合，我们将具有一可调整参数 $\beta \geq 0$ ，而其将被选择藉由控制权权重集中程度于最接近之配对组²⁵²⁶治理机制。

- 权重函数 1 (恒重)：

$$w(i) = \frac{1}{\# \{a_i \in A : a_i \neq w\}},$$

- 权重函数 2：

$$w(i) = \frac{\left(\frac{1}{|\text{margin of } a_i \text{ against } w|+1} \right)^\beta}{\sum_{a_j \neq w} \left(\frac{1}{|\text{margin of } a_j \text{ against } w|+1} \right)^\beta},$$

- 权重函数 3：

$$w(i) = \frac{1 - \left(\frac{|\text{margin of } a_i \text{ against } w|}{\text{total number of votes}} \right)^\beta}{\sum_{a_j \neq w} 1 - \left(\frac{|\text{margin of } a_j \text{ against } w|}{\text{total number of votes}} \right)^\beta}$$

²³ 此重新分配机制为启发由谢林币，详情请查看第 2 章节，而一陪审员将增加或损失其代币依据其投票是否与其他陪审员同调。请注意代币重新分配机制还正被积极研发且可能于未来继续演化发展。

²⁴ 如于一状态为无参与者投票同调，则支偿费用用途将被讨论检讨于治理程序。请参照第 5 章节来了解更多关于此的详细讨论。

²⁵ 请注意，一参与者可能会选择不同 β 依照何发生于各早期争议轮，此陪审员数量小到足以使 a_j 被狭隘决定且被高度权重为更加多变的，因此产生一定程度的随意性。例如，此可能极为帮助来考虑一先前讨论之上诉轮结果的边缘权重函数，因其可能将更佳适当反映社群意见。

²⁶ 请延伸注意无一考虑之权重函数将明确依赖选择之投票系统。于未来更进一步的开发中，聚合程序资讯导入于权重函数将有可能被实现，其中例如各轮任一可能选项被消除于 IRV-类型系统等资讯。

接着我们将评估此权重函数考虑利用以下特性:

	Winner First Max Payout	Unanimous No Weight	Concentration on Close Pairs
Weight Function 1	Yes	No	No
Weight Function 2	Yes	No	Intermediate
Weight Function 3	Yes	Yes	Better

- 赢家将首先获得一最大限度支偿 – 请注意, 所有权种函数将皆具有此特性, 而其确实遵照被提供于 2 章节的重新分配架构。然而, 一方能想像一支偿机制来不只依据投票者给予赢家选项 w 的相对位置, 其也将考虑投票者给予两非赢家选项的相对位置, 例如, 当一投票者选择来阶级排列 $a > b$ 或 $b > a$ 来为 $a, b \neq w$ 。从一用户体验观点来看, 我们将视其为重要的一点为来让用户不需要为认为非相关之选项来做阶级排列, 因此于所有我们的候选可能系统中, 此相对阶级排列将不会有任何权重分配。然而, 请注意此选择将基本上限制投票系统加上激励系统对于攻击之相对恒抗性。确实, 由 Arrow 的 Impossibility Theorem (不可能定理) 来说, 此为任何非平凡的投票系统, 且将会有一场合当”非关联代替”选项的相较阶级排列将会影响最终结果 [5]。为任何激励系统满足 Winner First(赢家首先)及 Maximum Payout(最大支偿)特性, 一投票者的阶级排列为此”非关联可能”方案将不会影响其支偿结果, 因此”微-贪腐”攻击的阈值, 如贿赂一陪审员来使其转换至相较无关系的选项之可能为较低。请参照 4.7.2.2 章节来了解为何此效应将可能被稍微减缓, 虽其还是存在, 此使用之投票系统将满足 Later No Harm(稍后无害)和 Later No Help(稍后无救)。
- 无权重之一致配对组 – 通常, 上述权重函数(除了恒重函数)为, 与 a_j 相比, a_i 将被赋予较多权重如相对恒与选项 w , 而与 a_j 和 w 相比 a_i 与 w 之距离将稍近。而如来讨论一极端状态, 一方可能会想要来希望一致相对抗的选项将被赋予零权重, 并不稀淡任何支偿系统效果来激励投票者来做出最正确阶级排列对于最相关联的选择对组。确实, 为一权重系统具有此特性, 如一非二元案例实际为一”拟二元”案例, 例如, 其具有两可能选项 a 和 b , 而所有投票者将 a 阶级排列首位且 b 次位于此顺位, 接着(假设此投票系统确实选择选项 a 或 b 为最终赢家, 而其将刚好为所有于 4.7.2.2 章节所讨论之案例) 只有 a 和 b 选项的相对恒抗将会获得一权重比例于激励系统内, 则此案例状态将被认定为于二元案例中所考虑到的激励范例。
- 集中权重于相近之配对组 – 此为比无权重一致性更平凡的情况。于先前讨论, 一方可能会想要来加权重于接近之配对组来增加攻击预防性。然而, 其可能还是会想要赋予权重至其他选项来激励投票者来谨慎的对待其投票权利(或至少对于预测之可能赢家选项进行阶级排列)。至少目前我们的评估对于不同权重于此标准为启发式的: 为使不同价值 β 及一常

见投票来分歧(例如, 2-1 分, 5-2 分, 或 12-3 分), 其需要多少权重赋予至各可能选项, 及此权重函数型态变化于 β 将影响治理 4.12 章节程序的柔软度来做调整。

于下列主张, 其能见识到此支偿系统将拥有许多良好特性来激励陪审员来阶级排列高顺度于期盼之可能赢家候选人, 应对至些许被列出于 4.7.2 章节的目标。

主张 1. 考虑此激励机制于此恒权重情况, 换言之, 权重函数 1 。假设一投票者得知一结果机率于投票结果公开前, 其为其他陪审员投票可能结果合各项案例上诉可能及赢出结果来计算可能发生的机率, 例如:

- 其相信于其投票轮中的其他陪审员将会独立考虑并与投票轮独立分开投票
- 其相信结果与其投票及其他陪审员的投票为独立分开事件
- 其配置可能结果 a_1, \dots, a_n 及可能性 $\text{prob}(a_1), \dots, \text{prob}(a_n)$, 为一期盼的赢出结果

接着一弱优势策略为此陪审员来提供一(严谨)阶级排列之结果 a_j 及从一最有可能来赢出的最高至最低机率于赢出 $\text{prob}(a_j)$ 机率。

请查看附录 A 为此证明结果。请注意从陪审员观点来看, 其投票将不会改变最终结果这点将能被道理化于我们的现有设定状态如所有陪审员深信一非正确结果将极有可能来被上诉。

于 Kleros 达成一决策后, 代币将被开放并重新分配至陪审员间。一范例之代币分配机制被呈现于图 10。值得注意的是, 此陪审员将可能失败来即时提示其投票决策。来避免激励此行为, 不投票场合之惩处程度必须至少与不同调投票相同。被激励的陪审员将永远尝试来提示其投票。于一上诉场合, 仲裁费和代币将被重新分配依照最终上诉结果。

当无攻击发生, 参与者为被激励来为其认同之, 其他参与方认同之诚实公平选项投票。于 Kleros, 谢林点为诚实且公平的。

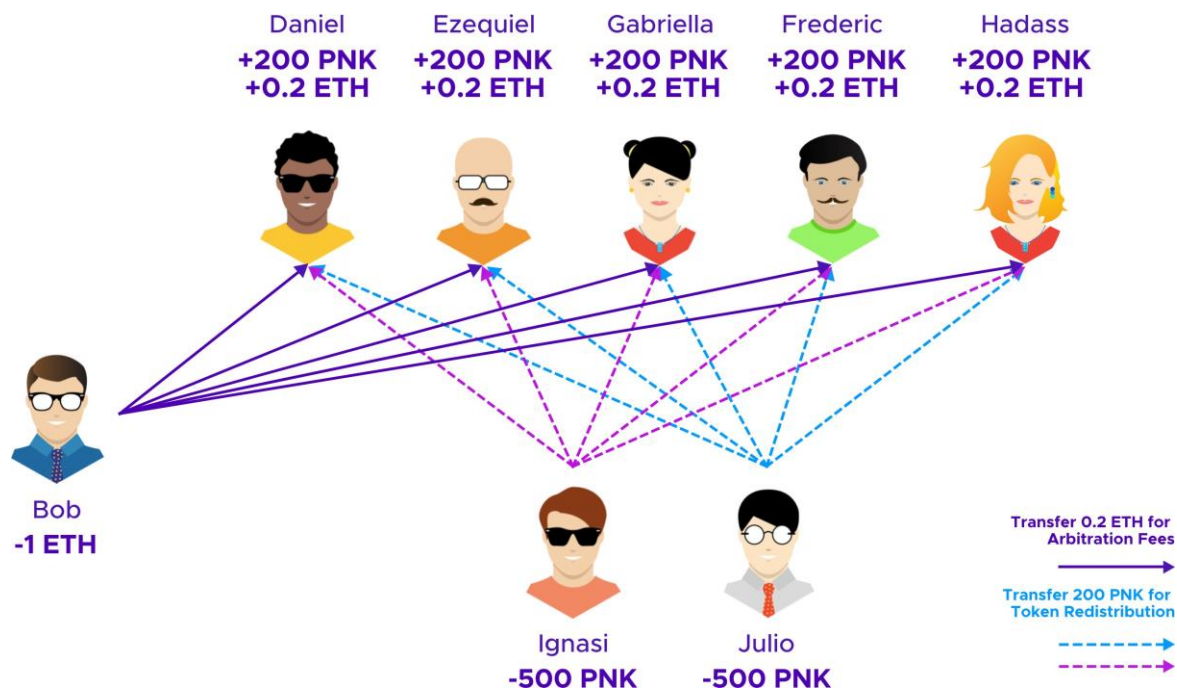


图 10：七个陪审员将于 Alice 或 Bob 中的选项中进行一二元选择。代币被重新分配从投票不同陪审员至投票同调陪审员。Bob 损失此争议并须支偿仲裁费。而另一方之汇款押金将被退款。

一方能争论此决策为十分客观的(相较与谢林币机制提供为一预测市场)，而无一谢林点将会产生于此状况。于 [55]，一非正式实验主导由 Thomas Schelling，而其展示于多数场合，被所有参与者来公同一致的谢林点并不时常存在。但 Schelling 发现，与其他选项相比，某些选项将更容易来被最终选上。因此即使一特别明显的选项并非存在，一些选项还是有可能被参与者视为较有可能的最终选出选项，而此类选项将会被最终有效选出。有时候，诚实陪审员还是也会损失代币。但只要长期总体来讲，其损失之金额量小于获赢之仲裁费加上从不同调陪审员方审议获赢之重新分配代币，其将代表系统还是为正常运作的²⁷。

备注 1. 于以上，我们见识到重新分配之仲裁费及损失之汇款押金将由各轮所处理。值得注意的是，如任一投票者察觉或怀疑其他投票者于其审议轮中已“非正确地”投票，其状况可能会更加激励其也来非诚实地来投票。于此极端场合，一单独同意最终结果之陪审员将可能获得全数仲裁费及损失之汇款押金于此轮，如其他所有陪审员与最终结果相异。我们也称此现象为“孤独的理性之声”效应。我们将延伸讨论此效应涵义于以下内容。

²⁷ 确实注意的是，此概念已大致正常运行于多数 [29] 考虑之实验场合，以及 [34] 及 [49] 的实际应用场合。

4.7.4 总结

考虑以上种种考量，为一涉及多重选项的典型案列，一良好的投票及激励机制似乎必须为：

- 投票系统 **WoodSIRV** (换言之，一方将使用阶级排列来模拟一系列之投票轮，并利用最少之首位排列来消除其他可能选项，如于 **IRV**，但于各轮开始前，其将查看其余的可能选项中是否可能有一孔多塞 (孔多塞) 赢家)²⁸。
- 权重函数 3 为，

$$w(i) = \frac{1 - \left(\frac{|\text{margin of } a_i \text{ against } w|}{\text{total number of votes}} \right)^\beta}{\sum_{a_j \neq w} 1 - \left(\frac{|\text{margin of } a_j \text{ against } w|}{\text{total number of votes}} \right)^\beta},$$

而 β 为一可调整的参数 (其能为任何随意一正价值数)。特别是，此权重函数应被计算基于上一投票轮的余量 (来使其基于一最大且最统计重要的样本) 当为投票者来计算奖励于案列轮早期。

尽管如此，些许特定之应用场合可能会想要来优先不同的特性取舍，如先前考虑的一样，而未来法庭版本之模组化架构将能使此应用来使用各自不同的投票及激励系统，甚至到一可能的替代架构型将被治理程序所批准允许之程度，详细请参照 4.12 章节。

4.7.5 仲裁费参数化

假设于一轮案列中我们有 M 个陪审员。一方必须选择 f ，而个人之平均陪审员费 (换言之，以让，体轮将需要 $M \cdot f$ 之仲裁费)，以及参数 α 和 min_stake (最低质押量) 先前介绍的一陪审员能损失的最大汇款押金量； $D = \alpha \cdot \text{min_stake}$ 。

再次，最终赢家结果将被表示为 w 。于此 4.7.3.2 章节之设计架构架构下，想像一诚实陪审员来花时间努力于 e ，且因此具有一结果为：

$$E \left[\frac{\sum_{a_j \neq w} \mathbf{1}_{\text{USR}: a_j < w} w(j)}{\sum_k \sum_{a_j \neq w} \mathbf{1}_{\text{USR}_k: a_j < w} w(j)} \mid \exists k: \text{USR}_k \text{ does not put } w \text{ last} \right] \geq \frac{1}{M},$$

即表示，于平均，其回馈量将至少与一平均陪审员回馈量相同。

再次，我们能表示 USR_j 的净回馈量为

$$\frac{Mf + \sum_k D \sum_{a_j \neq w} \mathbf{1}_{\text{USR}_k: a_j \geq w} w(j)}{\sum_k \sum_{a_j \neq w} \mathbf{1}_{\text{USR}_k: a_j < w} w(j)} \sum_{a_j \neq w} \mathbf{1}_{\text{USR}: a_j < w} w(j) - D \sum_{a_j \neq w} \mathbf{1}_{\text{USR}: a_j \geq w} w(j)$$

²⁸ 一重要技术性重点于投票选择系统为，如何处理平手状态。为 **WoodSIRV**，一从简化程式复杂性之简单选项将为要求一严密认定来赢取所有对抗场合之替代选项将被考虑为一孔多塞赢家，而当消除最后选项来为消除所有之最后平手选项。最后，一方能回覆“拒绝仲裁”，相似于目前替代机制来应对平手局面，如此程序导致所有选项被消除。然而，因此方案稍微与 **WoodSIRV** 普遍定义有些微不同，此可能导致某些于普通 **WoodSIRV** 中满足之特性来失败于一些极端场合 (例如，投票系统之克隆独立特性将可能发生如所有克隆组之参与选项平手于最终之投票轮)。

$$= \frac{Mf + MD}{\sum_k \sum_{a_j \neq w} \mathbf{1}_{\mathcal{USR}_k: a_j < w} w(j)} \sum_{a_j \neq w} \mathbf{1}_{\mathcal{USR}: a_j < w} w(j) - D.$$

表示

$$\pi_* = \text{prob} \left(\begin{array}{l} \mathcal{USR}_k \text{ puts} \\ w \text{ last } \forall k \end{array} \right)$$

接着，我们能计算一预计之价值于此诚实策略，基于上述之支偿范例：

$$\begin{aligned} E[\text{honest}] &= (1 - \pi_*) E \left[\text{honest} \mid \begin{array}{l} \exists k : \mathcal{USR}_k \text{ does} \\ \text{not put } w \text{ last} \end{array} \right] - \pi_*(D + e) \\ &= (1 - \pi_*) E \left[\frac{Mf + MD}{\sum_k \sum_{a_j \neq w} \mathbf{1}_{\mathcal{USR}_k: a_j < w} w(j)} \sum_{a_j \neq w} \mathbf{1}_{\mathcal{USR}: a_j < w} w(j) - D - e \mid \begin{array}{l} \exists k : \mathcal{USR}_k \text{ does} \\ \text{not put } w \text{ last} \end{array} \right] - \pi_*(D + e) \\ &\geq (1 - \pi_*)(f - e) - \pi_*(D + e). \end{aligned}$$

于另一方面，请注意，一特别案例当所有投票者于一投票轮中阶级排列 w 于最后选项将相对应的来获得一最低支偿，一对案例无具任何效益之”懒惰”策略被使用由投票者 \mathcal{USR}_i 将产生以下预期价值：

$$\begin{aligned} E[\text{lazy}] &= (1 - \pi_*) E \left[\frac{Mf + MD}{\sum_k \sum_{a_j \neq w} \mathbf{1}_{\mathcal{USR}_k: a_j < w} w(j)} \sum_{a_j \neq w} \mathbf{1}_{\mathcal{USR}: a_j < w} w(j) - D \mid \begin{array}{l} \exists k : \mathcal{USR}_k \text{ does} \\ \text{not put } w \text{ last} \end{array} \right] - \pi_* D \\ &= (1 - \pi_*) M(f + D) E \left[\frac{\sum_{a_j \neq w} \mathbf{1}_{\mathcal{USR}_i: a_j < w} w(j)}{\sum_k \sum_{a_j \neq w} \mathbf{1}_{\mathcal{USR}_k: a_j < w} w(j)} \mid \begin{array}{l} \exists k : \mathcal{USR}_k \text{ does} \\ \text{not put } w \text{ last} \end{array} \right] - D. \end{aligned}$$

只要最极具价值的”懒惰”策略具有一低平均支偿来提供为一平均陪审员，换具话说，只要：

$$E \left[\frac{\sum_{a_j \neq w} \mathbf{1}_{\mathcal{USR}_i: a_j < w} w(j)}{\sum_k \sum_{a_j \neq w} \mathbf{1}_{\mathcal{USR}_k: a_j < w} w(j)} \mid \begin{array}{l} \exists k : \mathcal{USR}_k \text{ does} \\ \text{not put } w \text{ last} \end{array} \right] \leq \frac{1}{M},$$

则其有可能来选择使 D 成为足够庞大来使”懒惰”策略具有一负期待回馈值。接着，一方应选择 f 及 D 来使：

$$(1 - \pi_*)(f - e) - \pi_*(D + e) > 0 > (1 - \pi_*) M(f + D) E \left[\frac{\sum_{a_j \neq w} \mathbf{1}_{\mathcal{USR}_i: a_j < w} w(j)}{\sum_k \sum_{a_j \neq w} \mathbf{1}_{\mathcal{USR}_k: a_j < w} w(j)} \mid \begin{array}{l} \exists k : \mathcal{USR}_k \text{ does} \\ \text{not put } w \text{ last} \end{array} \right] - D.$$

于此我们能检视

$$\pi_* = \text{prob} \left(\begin{array}{c} \mathcal{USR}_k \text{ puts} \\ w \text{ last } \forall k \end{array} \right) \text{ 及 } E \left[\frac{\sum_{a_j \neq w} \mathbf{1}_{\mathcal{USR}_k: a_j < w} w(j)}{\sum_k \sum_{a_j \neq w} \mathbf{1}_{\mathcal{USR}_k: a_j < w} w(j)} \mid \begin{array}{c} \exists k: \mathcal{USR}_k \text{ does} \\ \text{not put } w \text{ last} \end{array} \right]$$

- 为一能被任何法庭随时凭经验检视之数量值。

我们能进行相似分析基于 4.7.3.1 章节的提供模式。我们假设诚实策略将决定一赢出选项答案与一可能性 p 。假设所有除 USR 以外之其他所有陪审员采用此诚实策略，所以如考虑所有陪审员将单独选择其选项答案，此选择最终赢家答案之陪审员数量将会为二项式 $X \sim \text{Binom}(M-1, p)$ 。假设一不正确评价此案例之”懒惰”陪审员能来选择一正确答案选项与一可能性 $t \in [0, p]$ (例如，因为与业主方相比，法庭通常会偏倾向合约者方于一 t 部分比例之案件)。则：

$$E[\text{honest}] = pE \left[\frac{Mf + (M-X-1)D}{X+1} \right] + (1-p)(-D) - e = (f+D)(1 - (1-p)^M) - D - e$$

且

$$E[\text{lazy}] = tE \left[\frac{Mf + (M-X-1)D}{X+1} \right] + (1-t)(-D) = (f+D)\frac{t}{p}(1 - (1-p)^M) - D.$$

换言之，于此案例，以上限制将成为：

$$(f+D)(1 - (1-p)^M) - D - e > 0 > (f+D)\frac{t}{p}(1 - (1-p)^M) - D.$$

如以上所有条件满足，则此诚实选项为 Bayesian-Nash 激励机制可能。请注意于此于 4.7.3.2 章节的特殊案例中，陪审员将进行一二元选择，因此 $w(j) = 1$ ，而此双方设计架构相同。我们计算无陪审员投票为最终赢家之可能机率为 $(1-p)^M$ ，且

$$(f+D)(1 - (1-p)^M) - D - e > 0 > (f+D)\frac{t}{p}(1 - (1-p)^M) - D.$$

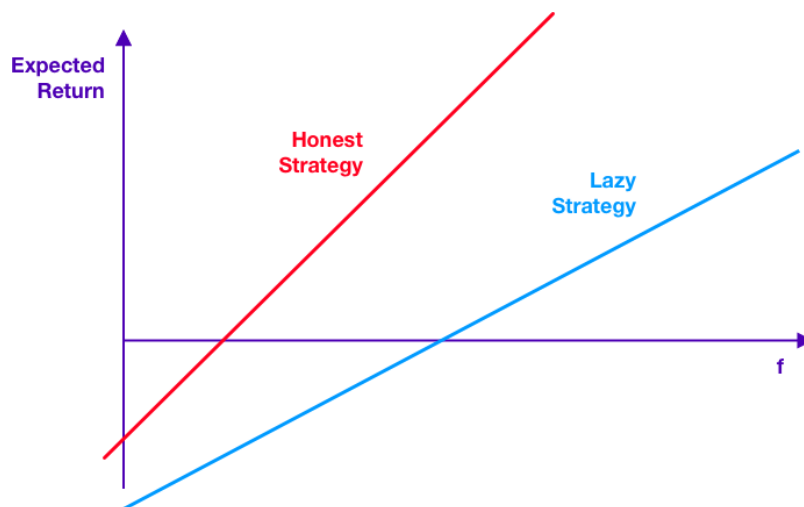


图 11：参数 f 和 D 应被选取来使确实努力来检视案例并诚实投票之策略将具有一正预计价值，且随意乱投票或持永远之投同一选项的懒惰策略将具有一负预计价值回馈。于此，选项 D 影响此曲线之位置，且能被选择当其具有一选取 f 可预计范围。

最终，此价值 f 和 D 将被选出藉由治理机制，详情请参照 4.12 章节。特别是，为遵循此推理逻辑，社群必须估计一价值如 e^{29} 。因此，如一合适数据为可用来合理化使用一更加细致之设计架构依据陪审员的付出努力相异于各人口结构，则治理投票将为负责来遵寻此论点之各微妙版本。

4.7.6 实施陪审员行为标准

些许方面的预测之陪审员行为，如承述于法庭政策，为客观的，而智能合约将无法具有能力来直接实施此类型行为。例如，当法庭政策可能需要陪审员来提供详细辩论理由为其投票选择，而其可能成为极为困难来使一自动化程序来辨别争论理由是否为一确实具有意义之理性叙述，还是一随机生成之文字串。相似之，此也极为困难来创建完全自动化之程序来适当反激励且预防陪审员来于投票期间中过早提示其投票结果，详情请参照 4.9.1 章节。

因此，未来 Kleros 版本将会使用 Kleros 自己本身能够来做出判断为客观性问题，藉由拥有一特别法庭来决定裁决关于一特定陪审员们是否确实违反相关法庭政策。而其即是，当于一包含延伸于既定投票期间的特定期限，一陪审员 Alice 将可被挑战争议如其投票行为于一审议中违反相关陪审员规范。此挑战将被分类于一分开争议，并被审议于一专属“程序法庭”。

不管挑战是否为成功与否，此挑战者将支付任何可能发起争议于程序法庭所需之仲裁费。而此挑战者将由可能赢取 Alice 的最低质押额的汇款押金机率来被激励接受此挑战花费成本。

其即是，为各法庭，其具有一参数 γ 选择由治理 4.12 章节。而如所有陪审员决定 Alice 违反相关法庭政策，此挑战者将成功获得以下额数：

$$\gamma \cdot \text{min_stake} \cdot \text{weight}$$

²⁹ 请注意，一方可能会想要不同案例只由一法庭所考虑来大致要求相似等级的努力付出程度并使陪审员无需只使用“诚实”策略为简单案例且“懒惰”策略于较难案例。尽管如此，即使案例于法庭为通常具有相当难易度，些许陪审员可能会还是需要与其他人想比较少之努力付出来成功做出一诚实裁决。

从 Alice 的质押 PNK。而如挑战者挑战失败，则 Alice 将获得此挑战者损失之挑战汇款押金。

4.8 上诉

如陪审团达成决策，而一方参与者感到不满 (因其认为结果为不公平)，其能上诉并使此争议被再次裁决。而这扩大之涵盖范围将通常具有一更高可能性来成为统计性代表为更广之陪审员社群。因为随着增加之陪审员数量，上诉之额外费用也必须被支付(上诉_费用 = 新_数量_陪审员 · 平均_费用_各_陪审员)。

此增加之陪审员数量将指数性增加当上诉场合发生；因此仲裁费也将随上诉次数而指数性增加。此代表，于多数情况下，参与方将并非选择来上诉，或只选择进行适量次数之上诉。因此，藉由上诉机制，Kleros 成功来避免大量陪审员需要考虑为同一案件之不必要的高成本重复劳动，而此机制也同时将预防降低攻击者贿赂陪审员至高次数上诉情况。

4.8.1 上诉法庭

于上诉情况下，一先前被考虑之案例将再次被考虑由一更加广大之陪审员参与，而于些许场合，此上诉能被提起至此法庭之”母法庭”，详情请参照 4.3 章节。

请注意，相较于”母法庭”，各”子法庭”普遍来说要求一更加精准之技术性技能。因此，当一案例进展至另一不同法庭，此将进入一陪审员可能较一般，且对于一特定案例用途具有较少技术性知识的法庭，而其将可能导致陪审员于母法庭需要花费更多努力付出来完成一正确质案/或获得一”诚实”裁决与一较低之一致性。但于另一方面，更多陪审员将质押于此母法庭；而其将获得更加强健之攻击预防性关于一系列不同之尝试攻击行为，详情请参照 4.11 章节。

因此，此不同法庭将展示一取舍介于专门技术性和攻击预防性。来使案例能持续来受惠于较技术性但较小之法庭，且同时成为攻击预防可能，法庭政策将需指导陪审员利用于上诉法庭来寻找任何可能之攻击证据。例如，普通法庭将包含以下指示：

“当考虑到一案例上诉情况于一较低阶层之法庭，陪审员应当来可虑 1) 评估此案例是否需要上诉法庭可能不会具有之特定技术性技能(例如：评价一英文至韩文之翻译品质，但韩文知识技能并非上诉法庭所要求之必备条件) 及 2) 其是否已有证据显示攻击正被进行于此较低阶层法庭案例(例如：贿赂攻击， $p+\epsilon$ 攻击，51%攻击等)。如其无任何可能之攻击证据且上诉法庭不能被预计来拥有一技术性技能来单独只为此案例进行评估，则陪审员们应当投票选择来执意于此较低阶层法庭之判决裁决 [39]。

此上诉法庭架构注重于程序问题，而其十分相似与上诉法庭的职位于如美国的联邦法院系统 [4]。此程序来提起上诉从一子法庭至其母法庭将能持续进行延伸至其案例抵达普通法庭。

于此目前设计架构，一上诉案例将”跳”至一更高阶法庭，则其即被考虑于其先前被考虑于先前被考虑之母法庭如：

$$\begin{array}{l} \text{number of jurors} \\ \text{in previous round} \end{array} > \text{threshold},$$

而此阈值为各法庭单独专属，且为藉由形容于 4.12 章节之治理程序所设置。当一数量之陪审员将与前一轮审议相较来加倍并加一于各轮，此架构将几本上决定多少上诉轮于一案例需要先被考虑

当移至后续应对之上诉法庭³⁰。如一数量之陪审员于此轮将超越普通法庭价值之阈值，则所有更进一步之上诉行为将导致一分叉投票，详情请参照 4.10 章节。

于未来之法庭版本，除了一超越阈值陪审员人数来传送一上诉至更高阶法庭之外，其也将具有一触发条件状况如：

$$\text{prob} \left(\begin{array}{c|c} \text{previous round} & \text{average juror would} \\ \text{result or} & \text{vote current winning choice} \\ \text{more extreme} & \text{first with } < \frac{1}{2} \text{ probability} \end{array} \right) \leq \text{threshold.}$$

此机率性将藉由二项式尾边界机制所预测。再次，此阈值为一个可调整之参数，而其被设置由形容于 4.12 章节之治理程序。此条件状况将允许一方来避免上诉于先前陪审员投票于此法庭已为过度压倒性且此统计性极可能之目前赢家可能选项也将代表一般陪审员意见于此法庭之法庭。

4.8.2 上诉费用设计架构和众筹

于现任版本之 Kleros，可被仲裁合约指定其设计架构来为收集需要之仲裁费用，并决定不支付此费用时需面临之连带后果。此各类设计架构将代表多项取舍抉择，而其将被讨论于下方章节。首先，一基本设计架构选项为：

- 于上诉之场合，一上诉人必须支付任何需要之上诉费。此具有一优势，于前一审议轮获胜之一方将不能于没进一步裁决的情况下败诉，换言之，其将不会败诉仅因其不欲支付上诉费用。于另一方面，此也有一忧虑，因为最终胜诉于上诉裁决的一方将不能获得其上诉费补偿，而此情况可能导致上诉程序只适用于相对来讲牵涉高价值的争议案例。
- 转之，双方将也可以事前被要求来支付一最低要求上诉费来涵盖必要花费，来以防万一如其败诉于一上诉场合。接着，如只有一方完成(全额)费用资助，则此方将无需额外上诉程序并自动成为默认赢家。来减缓前一审议轮之获胜者因只不欲支付适当上诉费用而自动败诉，我们要求上诉方来额外质押为此案例，其将高于陪审员需要之基本费用，而前一轮之获胜者将可能被要求较少量之此质押额。而此质押量将会用于来激励所有“费用资助者”。而此将激励第三方来为此选项支付上诉费用，特别是为前一轮之胜诉者。此架构相似与诉讼资金 [52]。值得注意的是，其费用能被一“团体”共同资助，详情将会被解释于下³¹。

于新一版本之 Kleros，此选项来决定何方能来支付上诉费及于何场合其将能支付上诉费之考量将被纳入至一仲裁方合约的设计中。然而，此版本法庭之模组化架构将能使参与方能够来自行选择从不同之上诉费用设计架构，只要其可能之设计架构已确实被批准由治理程序，详情请参照 4.12 章节。

³⁰ 请注意，介于治理程序来更新此阈值，一方能考虑为不同法庭之审员数量及多样化状况。特别是，一方能使用一较低价值于一较非技术性且较少特殊专精陪审员质押法庭之阈值。而其即是，一方能选择阈值来使更进一步之上诉于其法庭以低可能性地来抽选一提供一崭新案例分析的新陪审员，而案例将会进展至母法庭来被更加广泛的陪审员基层来做考虑。

³¹ 另一机制设计来保护可能无法支付一巨额上诉费用之经济资助性较差的参与方也为可能，且正被积极研究开发中。例如，争议方能参与一共同“上诉费用保险”。于此，参与方将汇款比前一轮陪审员费用还高额之押金当于创建争议初始期。接着此案例之败诉方将不会获得此差额，而其将被转至一资金池，而其将于需要之状况来为前一轮获胜者支付必要汇款押金。于不同设计架构，诉讼费用资金和费用保险将具有其各自取舍，但其也其实能被一起同时使用。

于此章节之剩余部分，我们将形容讨论些许机制，而于此第三方费用”资助者”将被激励来为争议方涵盖支付此上诉费。我们将能提供些许设计架构来为考量此，而其也再次牵涉到许多特性取舍场合。于设计此各架构，一方将必须考虑以下限制：

- 于一上诉轮的首发资助者必须质押于一提供之任一选项，所以如果其他选项没被费用资助，其将无争议产生且此质押选项将成为默认赢家。
 - 至少于各一轮，一资助者必须为错误的，所以其能涵盖支付上诉费用为此轮。
- 为下一章，我们使用以下表示符记：
- x 为后续上诉轮所需之陪审员总费用
 - S_{a_i} 为一高于仲裁费需要之额外质押，此为使来资助 a_i ；换言之，此总汇款金需要来资助 a_i 为 S_{a_i} ³²。

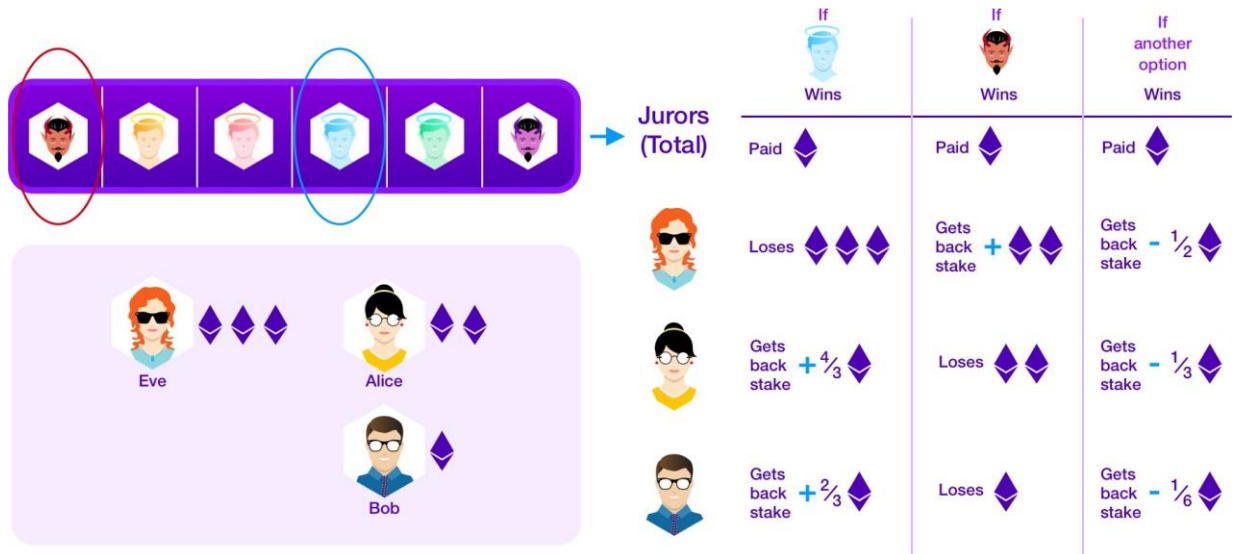


图 12：假设 Eve 资助上诉费用为一非诚实选项，Alice 和 Bob 将能筹资来资助上诉费用为另一(诚实)选项。众筹者将被激励来参与，因为其将可能赢取另一方将被要求支付之上诉费，而其额量将高于需要支付给陪审员之基本费用。于任何场合，当只有两选项被资助时将类似此模式，不管其使用何讨论于以下之众筹设计架构。

而不同设计将能被采用：

- 来资助一选项 a ，一方必须先汇款 $x + S_{a_i}$ 来使 a_i 被资助。而一旦两选项都被确实资助，一争议将正式产生。如其他另一方案最终获胜，此两资助者将平分负责此轮之仲裁费，否则其费用将被退款返回。我们将见识到此模式设计具有一定预防性为形容于 4.11 章节的”克隆资助”问题。然而，如多数选项被认为可能是诚实选项，则此设计架构将无法提供资助者来共同众筹资助的可能性。
- 于此上诉期间，用户能支付 $x + S_{a_i}$ 为一选项 a_i 来被资助。任何未被资助之选项将被于陪审员考虑选项中消除，其也包含未来可能轮次。此具有一之优势为，案例将于多轮小数量轮次进行后自行二元化，而其将移除拥有多项选项的复杂性。另一方面，主要通过要求支付

³² 此为可能于一上诉期间，而此治理机制为一法庭将修改需要之仲裁费用。一些选项来应对此，其为可能来从要求先前已被完全资助方来贡献更多切换至要求剩余参与方来贡献更多。

费用产生的风选结果将会冒着无一良好选项将会被成功资助的风险，而其将会可能使陪审员们被提供一无意义争议。更多的是，一方式来风选极度依赖支付费用之选项组将可能视为一富豪政治行为。除此，其也另有一可能不与现任仲裁方及可被仲裁方合约合作兼容的忧虑 [43]。

- 假设选项 b 获胜于前一之上诉轮。则一上诉将被调用如某些选项 $a \neq b$ ，及些许不包含 a 但包含 b 之选项组 S ，而 $x + S_a$ 将被质押于行为 a 由一或多的资助者，且 $r(\#S)x + \sum_{a_i \in S} S_{ai}$ 被质押于行为 S 由一或多的资助者，其中 $r(\#S)$ 为一渐增函数满足 $1 \leq r(\#S) \leq \#S$ 为所有价值 $\#S$ ³³。如 a 赢出，则 a 之资助者将获得其汇款押金退款加上基于其贡献比例来获得一部分 $(r(\#S) - 1)x + \sum_{a_i \in S} S_{ai}$ 。而如选项 S 赢出，则其选项资助者将依据其贡献比例来获得 S_a 。如一于 $\{a\} \cup S$ 之外的选项赢出，则 a 选项资助方将会获得其汇款金扣除 $\frac{x}{\#S+1}$ ，而 S 选项资助者将获得回其汇款金扣除 $\frac{r\#S}{\#S+1}$ 。如有其他能被考虑为诚实的选项，择此设计架构将赋予资助者们能共同资助来防备之可能性。然而，为一最简单选项 r ，且 $r(\#S) = 1$ ，其设计架构将于前任设计模式相比，具有较差的预防性对于”克隆资助”忧悲，形容于 4.11.4 章节。我们见识到于提案 7，如一方选择 $r(k) = \frac{k+1}{2}$ ，则此设计架构将具有于前任设计架构相同之克隆资助预防性，而同时能维持良好特性来使资助者们能共同进行闪躲机制，藉由添增之额外复杂性。
- 最终，我们将考虑一些微变化于前任设计架构，其中不同众筹者将能质押于不同选项组，而不是只有一选项组 S 被选择。我们利用 r 如上，一上诉将被触发如 $a \neq b$ ，则 $x + S_a$ 质押代表于 a 由一或多资助者，且其他非质押于选项不包含 a 之资助者将为

$$\sum_{\substack{S \subseteq A \\ a \notin S}} \frac{\text{Amount funded for } S}{\gamma(\#S)x + \sum_{c \in S} s_c} = 1. \quad (3)$$

接着回馈至多数参与者将为

$$\sum_{\substack{S \subseteq A \\ a \notin S}} \frac{\text{Amount funded for } S}{\gamma(\#S)x + \sum_{c \in S} s_c} \cdot \frac{\text{Return under prev. model if } S \text{ had been funded alone}}{1}.$$

特别注意，此支付给陪审员之额为 x ，且其关系为完全独立与何组选项被资助。除此，当 $s_c = S$ 为固定为所有 $c \neq b$ ，则以上之总和将能被有效计算出为参与资助者之总和，例如，公式 3 将成为

$$\sum_{\text{crowdfunder } \mathcal{USR}_j} \frac{\text{Amount funded by } \mathcal{USR}_j \text{ for } S_j}{\gamma(\#S_j)x + \#S_j \cdot s + (s - s_b) \cdot \mathbf{1}_{b \in S_j}} = 1.$$

我们将看到此设计架构带有多项设计架构的优势，当单项选择组 S 被资助，此提供更多柔软性为众筹资助者来质押于不同选项组，且也提供一选择来能够共同资助一上诉。

³³ 请注意，一兼容之组选项 S 能被发现存在如所有选项 a_i 或至少 S_{ai} 已被提出。

于此所有设计架构，如不足够资金被筹募为一选项或一组选项，此筹募之资金应被归还至其最初贡献者。此激励资助者来参与于此程序，并同时能够避免不必要之风险关于此选项将最终到底会不会被资助。

备注 2. 请注意于我们的以上设计架构，我们允许一可能来使些许于同一“侧”之选项被同时资助。理想状况下，一方能进行任何精细计算来“赌注”于任何一争议“侧”，或如真有必要，资助一双方综合选项结果来做为保险。然而，于先前提及之限制，此首被资助之争议选项“侧”将必须代表一默认赢家如无一其他选项被资助费用。一方能想像某人可能会尝试来巧妙地利用适应此规则，例如使用前一轮中阶级排列最高一选项来与其他共同资助之选项互组成为一默认选项。而此将成为非常脆弱对于攻击如已成功贪腐前一审议轮之恶意方能保证所有高阶阶级排列之选项为实际上恶意选项，并接着将其中一高阶阶级排列的非诚实选项与其他足够数量之诚实选项组来互组并使其不意察觉，最终来让其他诚实参与方来无法资助一另一异侧选项来产生一争议场合。

备注 3. 此众筹机制并非能使完全上诉费用惠实易人。虽(不同)资助者能涵盖支付费用为任一争议侧，此还是为一负总和游戏场合来相互意见对抗因资助者必须共同支付仲裁费用为一上诉轮。特别是，资助争议双侧通常只可行于一场合当资助者具有一非常不同之优先可能性判断对于各最终结果选项。确实，其通常会有一范围系列之资助者先验为一非能清楚来判断应资助于何侧选项的争议案例。此问题将急遽发展当一数量之可能结果开始增生；而与一多重选项，一攻击能轻易将易争议推向明显是错误选项且不会面临到任何一诚实选项具有足够机会来被成功资助于上诉。此场合特别为真当克隆选项开始降低任何诚实选项将赢出之可能机率。因此，当设计一可被仲裁之合约时，一方应当考虑来结合一众筹利用执案前置上诉费用保险，并细心检视可能之所有可能提议结果，并避免任何可能的克隆选项。

4.8.2.1 同时资助数组选项

我们将简单显示一些关于以下多重组选项被共同资助之场合结果，换句话说，此为以上讨论之第三和第四设计架构。其中特别，我们见识到参与者资助一不会伤害到其他已(部分)资助参与者之一另外选项。我们能首次看到其将合理化为一侧选项之资助者来为其他不同选项进行资助因为其能维持正预期价值回馈并同时减低变动性。

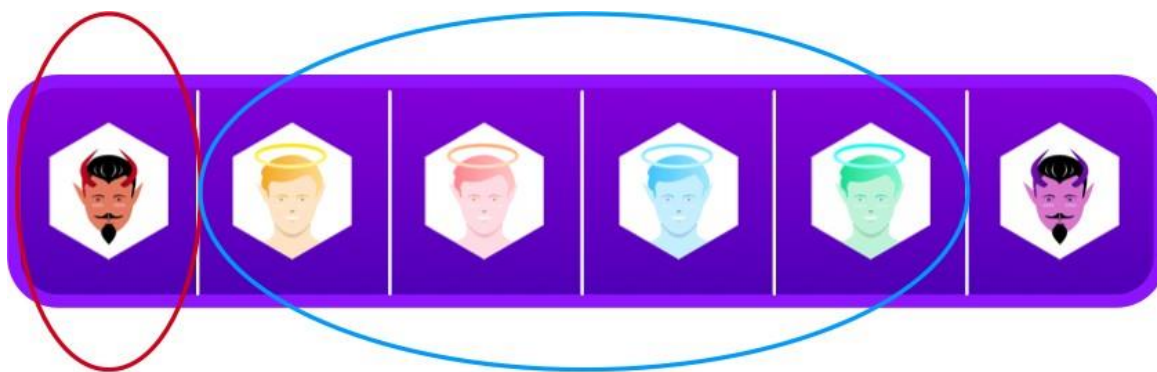


图 13：当一方使用上述之第三或第四众筹设计架构，则资助者将能资助费用为一组选项们。于此，与图 12 的情况相反，众筹者将共同质押于诚实选项并获胜如其中任一选项最终赢出于此

争议。相较于只有一选项被资助之情况下，此将需要更一庞大的众筹者总体贡献，然而，通常此额外费用成本来添增一选项具次添加性，而此添加性将控制由选项 r 。此使一形式之对冲保障来足以维持众筹之有效性，即便于一克隆选选项存在之情况。

主张 2. 假设函数 r 具有一特性 $r(n) + r(1) \geq r(n+1)$ ，为所有 $n \in N$ 。接着假设一数组结果 S 具有一非负预期价值且单独资助一结果 a_j 具有一非负预期价值，且资助 $S \cup \{a_i\}$ 总和来说具有一非负预期价值。

证明。 假设 a 为一选项资助由一反对侧。 $\#S = n$ 。则

$$E[S \cup \{a_j\}] \geq E[S] - E[a_j] \Leftrightarrow$$

$$p_a x (-\gamma(n+1) + \gamma(n) + \gamma(1)) + (1-p_a) \left(\frac{nx}{n+1} + \frac{x}{2} - \frac{(n+1)x}{n+2} \right) + \sum_i p_{a_i} \left(\frac{(n+1)x}{n+2} - \frac{nx}{n+1} \right) + p_{a_j} \left(\frac{(n+1)x}{n+2} - \frac{x}{2} \right) \geq 0.$$

基于我们的假设 r ，此首先项目将成为非负价值。其他项目也明显非负价值因 $n \geq 0$ 。

主张 3. 假设资助一具有非负预期价值之 a 选项对方侧已资助 a_j 为任何选项结果 $a_j \in S$ 。则此资助将具有一非负预期价值如反对侧已共同资助 S 。除此，于上述之第四设计架构，如资助一选项 a 具有一非负预期价值当反对方已资助 S_j 为任何 S_j 并让 $a \notin S_j$ ，则资助一选项具有一非负预期价值为公式 3 成立之任何质押选择。

证明。 让 $n = \#S$ ，接着让 $n \geq 1$ ，

$$E[a] = p_a \left((\gamma(n) - 1)x + \sum_{c \in S} s_c \right) + \left(\sum_{c \in S} p_c \right) (-x - s_a) + \left(1 - p_a - \sum_{c \in S} p_c \right) \frac{-x}{n+1}.$$

接着让 $n \geq 2$ ，

$$E[a] - E[a : \text{remove } c_1 \text{ from } S]$$

$$= p_a (\gamma(n) - \gamma(n-1)) + p_a s_{c_1} + p_{c_1} (-x - s_a) + \left(1 - p_a - \sum_{c \in S} p_c \right) \frac{-x}{n+1} - \left(1 - p_a - \sum_{c \neq c_1 \in S} p_c \right) \frac{-x}{n}.$$

当 $p_{c_1} \geq 0$ ，

$$\left(1 - p_a - \sum_{c \in S} p_c \right) \frac{-x}{n+1} - \left(1 - p_a - \sum_{c \neq c_1 \in S} p_c \right) \frac{-x}{n}$$

为清楚的是非负价值。然而，

$$p_a s_{c_1} + p_{c_1} (-x - s_a) \geq E[c \text{ against } c_1] \geq 0$$

之一假设。

除此， r 将由假设情况下持续渐增。一方能具有一完整争论藉由使用一 $n = 1$ 案例场合为

$$E[a \text{ versus singleton}] - E[a \text{ if opposition unfunded}] = E[a \text{ versus singleton}] \geq 0$$

一假设。

为第二宣称，我们将看到

$$E[a] = \sum_{S_j} \frac{\text{Amount funded for } S_j}{\gamma(\#S_j)x + \sum_{c \in S_j} s_c} \left(p_a \left((\gamma(\#S_j) - 1)x + \sum_{c \in S_j} s_c \right) + \left(\sum_{c \in S_j} p_c \right) (-x - s_a) + \left(1 - p_a - \sum_{c \in S_j} p_c \right) \frac{-x}{\#S_j + 1} \right).$$

然而，我们必须拥有

$$p_a \left((\gamma(\#S_j) - 1)x + \sum_{c \in S_j} s_c \right) + \left(\sum_{c \in S_j} p_c \right) (-x - s_a) + \left(1 - p_a - \sum_{c \in S_j} p_c \right) \frac{-x}{\#S_j + 1} \geq 0$$

为一假设为所有 S_j ，而因此 $E[a]$ 为一所有非负价值之数量总和。

所以，而上述第三及第四之众筹设计架构，我们的预期行为，针对必须最为使单一选项被资助的资助者方，其考虑选项将为其认为最终赢出机率最大之选项。其将接着期盼其他资助者将不会资助相似选项或”克隆”选项³⁴。因此，资助者将倾向来成为默认赢出，或成为相对抗与其资助之选项大大不同之其他选项(们)。此主张 3 将为我们显示如一资助者 **Frederick** 认为，与其他选项相比，一选项值得来被单独投保，则其将还是会为值得来投保即便 **Frederick** 与其他共同选项有需许对抗。于另一方面，遵循主张 2，只为群体侧资助一小部分费用的资助者将可能理性地来资助一或多选项，并使其于一多变场合最为对抗选项且保障些许预期回报。

³⁴ 资助此克隆选项将拥有一负预期价值回报，更多详情分析关于此主题，请参照主张 7 于 4.11 章节。然而，一攻击者可能会愿意来接受一负预期价值回报来足以”忧悲”诚实资助者藉由同时减低其预期回报。请注意，如所见于主张 7，如一可能克隆选项数量为低数值，则此”忧悲”行动将无法有效来达成其目的。

4.8.2.2 众筹设计架构的各项取舍

考虑到于 4.8.2.1 章节所考虑到地种种特性，我们为上述之四门主要众筹设计模行总结些许不同之优势及劣势。

设计架构	优势	劣势
需要两选项被各自资助，不会消除其他选项	<ul style="list-style-type: none"> • 简易 	<ul style="list-style-type: none"> • 十分脆弱对于无一选项被资助及/或资助被分割于多选项之问题情况
只资助被陪审员考虑于后续轮中被考虑之选项	<ul style="list-style-type: none"> • 较不容易发生策略性投票影响于拥有较少选项之后续轮中 • 对于无一选项值得来被资助之情况拥有较强之应对预防性 	<ul style="list-style-type: none"> • 无一自然方式来质押于多重选项，因此较差效应对于诚实资助者代币流动性被分割至多重选项 • 易将系统推向复数决，因陪审员需要考虑所有可能被资助之选项 • 如无一优良选项被资助于此轮初期阶段，不合理的奇怪问题被提供至陪审员的机率将会大幅增加
一选项(a)必须被完全资助，接着另一侧陪审员将质押于一选项组 S	<ul style="list-style-type: none"> • 资助者(选项 a 以外)能进行更高额质押，并解决代币流动量问题 	<ul style="list-style-type: none"> • 不对称性将发生于资助于争议的两侧，一侧可能必须一单独选项，而其可能混淆用户体验 • 复杂化用户体验，因众筹者必须表明其资助意愿对于不同选项组
一选项(a)必须被完全资助，接着另一侧之陪审员将质押于一选项组 S_j ，而其并非全数一致	<ul style="list-style-type: none"> • 资助者(选项 a 以外)能进行高额质押，并解决代币流动量问题 • 要求各众筹者来特定表明一单一选项组 S_j，而与前述设计架构相比，其将简化用户体验 	<ul style="list-style-type: none"> • 不对称性将发生于资助于争议的两侧，一侧可能必须一单独选项，而其可能混淆用户体验

4.8.3 参数化质押

於于 4.8.2 章节，我们见识到资助者来资助为一成功上诉的回报将依据此需要支付给陪审员的仲裁费以及争议资助者双侧需支付之额外质押数。此质押选择于任何一应用场合将依照使用之可被仲裁合约。于此章节，我们将来进行些许有帮助的观察对于如何选择各类选项。除了上轮获胜之选项外，我们通常将使需要之质押量相同为全数选项。而前一轮获胜之选项将可能要求较少质押量。而第一个众招设计架构下，当只有两选项能被资助，则资助获胜于前一轮之选项 b 将具有一正预期价值如果：

$$E[b] = p_b s_a + p_a(-x - s_b) + (1 - p_a - p_b) \frac{x}{2} > 0$$

为任何选项 $a \neq b$ 。而如果我们想要来选择质押以让其能永远值得来资助一前一轮赢家而此也将被一资助者来预测成为一最具有机率来赢出的选项，此方能假设 $p_b \geq \frac{1}{n}$ ，其中 n 为总可能结果数量。接着以上之不等式将成立如：

$$s_a > s_b + \frac{nx}{2}.$$

即表示，质押需要为前一轮之败诉者将应当被选择按照前一轮之赢家质押要求量³⁵。接着，与一相似点：

$$E[a] = p_a s_b + p_b(-x - s_a) + (1 - p_a - p_b) \frac{x}{2} > 0 \Leftrightarrow p_a > \frac{p_b \left(\frac{x}{2} + s_a \right) + \frac{x}{2}}{s_b + \frac{x}{2}},$$

一方能选择 s_a 来使非前一轮之获胜者为可保证的于一阈值 p_a 。

理由为此另一众筹设计架构也非常相似。于第三合第四的设计架构中，此为可能为只有一选项将被资助于 S 中。基于主张 2 和 3，此能被视为一最不理想之场合来激励费用资助者。因此，此为很自然来要求相同质押量于此场合来与前一设计模型额数量相同。为第二设计架构，其基本上消除所有未被资助之选项，而一方可能会想要来资助一于前轮获胜之选项 b 来获得一正预期回报，只要 $p_b \geq \frac{1}{\#S}$ 为任何被资助之组 S 选项。接着，所有除了 b 以外之选项将要求一质押量 s ，来有效具有：

$$E[b] = p_b s \#S + (1 - p_b)(-x - s_b) > 0,$$

为此，我们将见到此为足够来拥有 $s > x + S_b$ 。

³⁵ 请注意此类不等式可能结果数量之线性依赖性。此可能为非合适为一巨额结果，特别当一方可能选择质押来使只有前一轮获胜者将被保证一正预期回报如其为具有一较高获胜机率。例如，如一方假设 $p_b \geq \frac{1}{2}$ ，则 $s_a > S_b + x$ 为足够。或者，一方能稍微调整此设计架构使当 a 或 b 都没胜利时，前一轮获胜之资助者将获得其全额汇款押金退款与一额外送至资助其他选项之资助者的仲裁负担。此有一优势，其质押间关系将不被继续依赖于 n ，但以一使前一轮败诉者甚至更加不利并添增程式设计的牺牲代价。

4.9 预防提前揭示陪审员投票

4.9.1 投票承诺和揭示

于 4.7.1 章节，我们表明陪审员将“投下”其票介于一投票期间。即是，其将提交一哈希(投票，随值，地址)，并接着于投票期间结束后，其将有一揭示期间来使陪审员来公开其投票及随值。于此章节，我们将详细叙述此程序为一部份讨论关于广泛机制对于如何来限制陪审员的投票资讯循环于系统内介于投票期间。

此随值为一随意生成价值来使添加内定性来预防彩虹表的使用³⁶。介于一投票期间，陪审员能重复其承诺程序来重新提交一新承诺投票。此投票将成为可能与前一承诺相同但与一不同之随值，或其可能为一完全不同之投票。此承诺期间结束前接收之最后承诺将被用于投票聚合及激励，而其前任投票将被废弃。然而，假设标准之共谋攻击预防特性 于哈希诚实性，陪审员将无法生成一清楚决定投票和一组生成相哈希之随值。因此，陪审员将无法变更其投票于各承诺轮结束后。藉由此程序，其他陪审员或任何一参与方将无法来看见此投票。此也将预防一陪审员之投票结果来影响其他陪审员投票。

4.9.2 惩处过早揭示投票之陪审员

于上述我们介绍来使陪审员能保密其投票结果至所有陪审员投票承诺完成的投票承诺及揭示架构。然而，此架构并非能自行预防陪审员来非理性地乱公告其投票来尝试影响其他陪审员。至一定程度，一方将可能不会预期来视一特定陪审员的投票极为信服，即便此投票结果可能拥有公开之多数性于此目前进行轮，而如此为一非诚实投票结果，投向少数诚实方陪审员可能将预测来拥有一可能之上诉轮。藉由一讨论于备注 1 之”孤独的理性之声”效应，其解释其实当知道于此轮之投票者投票”错误”时，其将赋予您更多”激励”来正确投票。

我们讨论如何延伸来逆向激励陪审员来不要提供任何投票情报。请注意，提供可信情报关于一方之投票选项将可能存在于下列几种型态：

- 陪审员公开其投票承诺之相对随值
- 陪审员能送发一 **ZK** 证明(零知识证明)关于其某一方式之投下之投票承诺
- 陪审员能自行创建一智能合约来承诺至一投票，而此合约将销毁其汇款押金如投票行动与定义之不符。

基于多样化之策略方案来供陪审员选择来提前接式其投票，此极为重要来拥有一完全自动化之方式来惩处进行此之行动方(例如，一机制来惩处一方之 **PNK** 质押如其投票随值被提供于投票截止前)。反之，于未来版本之 **Kleros**，提前揭示投票将成为一可能被挑战于程序法庭之陪审员行动，详情请参照 4.7.6 章节。

³⁶ 一目前被导入于 **Kleros** 用户介面的机制，随值为被生成利用其以太坊密钥来签署包含一特定争议辨别者之区块文本。接着此随值将随时利用主钥来签署与相同文本来进行恢复。尽管如此，利用不同钥键于此相同文本之签章将也为不同，而于一签署演算法之假设情况下，如一方无此用户之密钥，则其为计算性非可能来获得此签章。因此，一名陪审员将有此机制来被预防克隆复制其他陪审员的投票承诺。但相反之，如一用户删除其随值于其当地记忆体，其能重新生成此只要其还确实具有其密钥。

我们正持续来积极研发其他预防方案来融于未来版本之 Kleros，而其包含基于反提前揭示游戏 [16]³⁷之方案，以及参考共谋预防 [19]³⁸的主意想法。

4.9.3 自动化投票显示

当承诺及揭示投票之此两步骤，形容于 4.9.1 章节，需要额外之用户互动，于一些低质押量法庭，一方可能会想要投票来被公开以便简化用户体验。正如形容于 4.9.2 章节，Kleros 正使用一上诉系统之事实表示，即便一多数投票于一投票轮已被投下为一特定选项，投下那特定选项也不一定代表其将必定保证此选项将成为最终被用于代币重配之最后选项。此特征限制投票克隆策略的有效性，而使公开投票或许成为可接受的方案于一些案例场合。使用何系统架构将被决定藉由法庭参数，详情请参照 4.12 章节关于治理之部分。

抽象的来说，一方可能希望拥有一机制来使投票自行来”揭发自己”于一指定时间，无需任何用户行动牵涉。不幸的是，当一无信任第三方来记录投票且加速其步骤，此为极为困难来达成于一去中央化系统。些许可能方案为：

- 来使一浏览器扩张或应用程式于陪审员设备端来存储此投票及随值资讯，并将此释出于一合适期间。于此情况，只有用户个人(及其设备端)将能知道其投票于揭发期间前，而尽管如此，为避免繁杂用户体验，其将要求陪审员来积极向自行提交一第二笔交易。请注意，然而，而此方式下一用户将需要来极为小心来使其设备端确实为开启状态介于一投票揭示期间。
- 来使用一阈值加密 [48]。于此陪审员投票及随值将被加密利用与一包含 n 人数成员团队之公共钥，而任何团队中 t 人数来共同合作，其将能来成功恢复此团队之密加密钥及解密。请参照 [57] 来为此主意之目前导入于以太坊。虽此方案将加强一额外之管控，特别是关于补偿阈值加密之参与者。

此方案将可能会被使用于未来，以便简化用户体验并同时使一方能更广泛地进行投票承诺及揭示于不同法庭。请注意，至少于一陪审员以外之第三方地址能提交投票之一定程度，随值资讯将以一揭示交易介于揭示期间，而从一法庭智能合约的观点来看，此将不会要紧关于最终究竟使用何方案。因此，无论何机制最终被使用来使投票及随值可行化介于揭示期间，此机制可被设置作为一既存法庭合约之覆盖机制层。

4.10 分叉

一拥高比例 PNK 额量，但还是失败于一 51%攻击案例之攻击者将丧失其部分之质押量当被每次抽选。然而，因只有一组选项数量之 PNK 将被抽选为一特定案例，即使于一上诉轮，此攻击者也将只会通常损失一全体持有量中一小额量之损失汇款押金。来使最大化 51%攻击之成本，于此章节

³⁷ 于反提前揭示游戏如考虑于[16]，用户能放置赌注于陪审员投票及被回报于陪审员汇款量的押金额量或对于各选项之投票者来依据决定之陪审员补偿额量。其被校准于此方式来使用户能只接收一正预期价值回报藉由下注于陪审员投票至一定程度至其具有一定些知识关于单体陪审员将会投票超越接受更多平均投票之广泛趋势。

³⁸ 于一共谋预防机制，陪审员将不应当能可信地来证明其他人之特定投票方式，于理想之情况下，其其实也不应该能达成此于案件解决后。此特性将还具有抑制贿赂攻击之作用。请注意，于未来版本之 Kleros，陪审员于投票期间来重新投票承诺至一不同选项之能力，与只有最终投票被采用，将基于共谋攻击之精神 [19]。尽管如此，此并非提供一完整共谋预防因陪审员还是能够于投票期间后证明公布其如何投票。而确实，当陪审员接收相异支偿以其一投票函数功能，其极为困难来建立一系统来使无人能提供证据来公开表示其投票方式，即便于一案例结案及支偿重新分配之后。

我们将提倡一”终极投票轮”来使全数 PNK 持有者来进行投票。此后发由一相似机制于 Augur [49]，但适应至 Kleros 使用的情况。

此主意为一方能进行”分叉”，创建两版本之系统各自依据一持续之特定投票结果，而攻击者持有代币之分叉，将被广泛市场视为一恶意分叉，而与其他”诚实”分叉相比，其代币将不会被考虑来具有任何价值。于目前开发阶段，此并非有一正式机制来加促进分叉，然而，其将不会有任何阻碍来阻挡社群成员来克隆 Kleros 并使一持续决定之结果被逆转且尝试来建立一社群共识环绕来使此复制主版 Kleros 之克隆系统来能够持续进行。剩余章节部分将详细解释将可能来促进环绕一分叉系统的整体社群所需之特性机制，而其将被讨论于下。

Kleros 的一重要特征为案例时常极为客观的。因此，此很有可能发生当陪审员真心无法同意之场合情况。而确实，我们能想像一后续上诉轮的狭隘结果将很有可能成为以下之任一结果现象：

- 一尝试之 51% 攻击来欲使一明显之非诚实选项来胜出通过。
- 一深度意识形态分裂对于特定案例之判断³⁹。
- 一诚实意见分歧对于一特定案例之具体细节，其将对未来案例几乎没有影响。

于以上之第一情况场合，一方可能会想要有一分叉来移除攻击者之影响力；于第三情况场合，一方可能不会想要有一分叉因其可能导致不必要之分裂于既有社群内部。一基于意识形态分裂之分叉可能被正当化，依照社群整体如何评断此意识形态差别程度。来决定究竟于何一场何情况，于我们的”最终分叉轮”，PNK 持有者将表明其投票意见，加上其想法认为此案例究竟值不值得来进行一分叉执行。

当然，一系统机制使用虑多数来考虑关于是否值得来分叉将成为无效果的当面对一成功之 51% 攻击，因此攻击者已控制双侧投票之结果。反之，PNK 持有者能特别定义当一部分比例之全体 PNK 额量将成为分叉，其也将愿意一同进行分叉。则任一 PNK 持有者将能设置此比例设定并使其剩余之代币将待在于主分叉不管结果如何，也不管其认为此结果是否为一诚实之意见分歧场合，且其是否认为其能必定来避免一成功之 51% 攻击。或是，PNK 持有者能设置此分叉额量比例至一中等数量价值，以便其只会分叉当其具有一足够支持方，且其赞同之意识型态群也将有足够能力来维持使此分叉能持续可行。我们设想编辑可被仲裁合约于一想法方式，其为对于意见一致相同之多方关心者，此一仲裁者为此特定合约能被取代藉由一 Kleros 分叉。因此，此限制一成功之 51% 攻击者来挟持 Kleros 用户的可能性，除了当攻击者具有一较直接之利益考量之一些相较珍奇的状况。用户介面能警示参与方关于此分叉发生并告知其分叉之产生原因。

4.10.1 分叉机制

我想像任一代币持有主之效用对于任一可能分叉之案例为一功能函数：

$$\text{utility} = \text{fct} \left(\begin{array}{l} \text{case outcome} \\ \text{on the fork} \end{array}, \begin{array}{l} \text{percentage of tokens that are on} \\ \text{the same fork as me after the case} \end{array} \right).$$

³⁹ 例如，一文字主义者/规范精神者的分裂类型，视于 Augur 的”谁将控制美国参议院于期中选举后”类型市场如其已进行发展一段时间足够来进行一分叉 [45]。其也比较于以太坊/以太坊经典分叉关于如何应对 DAO 骇客事件。

此为可能来允许一取舍对于此赢出选项为究竟多不正确/不可接受，且一分析关于此导致社群如何分裂。我们能想像一案例当某人认为一结果 a 为相当不公平，而其将可能具有价值来分叉至一 b 为赢家之平行宇宙，但其将只会实际进行分叉如一定之社群比例愿意与其进行分叉。否则，如只有少数社群愿意对于此案例进行分叉，其将选择来容忍此结果 a 并持续来存留于主支系统⁴⁰。

我们能预期此效用函数将为单调效能来对于与您进行相同分叉之代币比例额。即是，其他所有情况条件为平等一致，则我们将假设参与者将不会想要其欲想参与之分叉为较小规模之分叉，因其将一程度意表此分叉可能将具有较低机会来持续进行发展。此相互动情形有点类似于博弈理论中“两性之战”之合作问题，当两参与方尝试来合作协调于两可能结果，而虽其具有相异之偏好结果，其最终将通常拥有一共识之相同结果，因为其中一方将即有可能为较强之方，而其偏好选项将成为最终整体之偏好选项。

因此我们提出以下建议：当一案件已被上诉至一最大限度次数，一最终投票轮将被触发且使所有 PNK 持有主来参与⁴¹。各 PNK 持有主 USR_i 提交 $(a_{ij}, r_{ij}^0) \in L(A) \times [0,1]^n$ ，为 $n \leq \#A$ ，其包含一阶级排列投票 $a_{i1} \geq a_{i2} \geq \dots$ 受制于的约束 $r_{i1}^0 \leq r_{i2}^0 \leq r_{i3}^0 < \dots$ ⁴²。此用户之选项 r_{i1}^0 将基本上使其将能指定依最低阈值为社群支持度关于一分叉，当 a_j 被考虑成为赢家而 USR_i 将会想要加入此分叉⁴³。

此一“主分叉”；为当结果 a_{main} 应对于选项被选择为“赢家”来安局任何 ETH 支偿于此案例，以及，于一默认设定，于其他既存合约。此赢出选项将被选择如下：当参与者提交阶级排列选项 r_{ij}^0 ，一方拥有足够资讯关于投票偏号来使用此相同系统于 4.7.2 章节来决定一赢家于此“最终分叉投票轮”。接著任何投票者表示此 a_{main} 为“可接受的”藉由包含其阶级排列将自动持续存留于主分叉。

于各分叉，赢家于其分叉将来重新分配 PNK 为于前一轮同调将成为一选项被选择于此分叉。因此，如一陪审员于一早期轮坚信一决策需要一分叉轮，且其相信其将有自信来选择此 PNK 还会具有市场价值之分叉，其被讨论于 4.7.3 章节的理由关于如何激励为前一轮将持续有效。请注意此为可能使 PNK 来“丧失”给 Bob 于一场合当 Alice 为非同调之分叉仍然于一 Alice 为同调之分叉之上。于另一方面，我们将不会重新分配为同调 PNK 持有者之“投票”于一分叉轮，除非 PNK 持有者们将最终决定其结束于何分叉⁴⁴。

⁴⁰ 此可能同时抽想化其预测随案例进行之代币价格变化，以和其道德/利他主义及愿意性来参与于一其视正义或非正义之系统。

⁴¹ 请注意，于一定程度，此分叉程序形容于此将促进一原先协议之外可能的社群的社交共识之相同程序。于一社交共识分叉之案例场合，此也很可能来为使一子组社群来发现一结果将最终赢出(或已赢出)，并以一无需等待或支偿上诉费的情况下进行一多次上诉。于未来工作研究，我们将考虑如何来扩展此分叉机制来使一群体能来协调合作环绕一分叉于一早期上诉轮，因此促进一广泛健康的社群场合来使共识分叉来足以进行发展。

⁴² 此并非最佳表达方式；一投票者将可能愿意来分叉至一 a_1 ，以一与 a_2 相较下较低支持度，但尽管如此，其愿意来成为一“较大”之分叉至 a_2 而非一“较小”之分叉至 a_1 ，而此为一较不容易来意表于此设计架构之偏好。然而，一较丰富的表达将需要一较复杂之用户体验，且可能需要一较久运行时间来解决此问题。

⁴³ 请注意一用户特定指定出 r_{i1}^0 作为阈值来作为一分叉支持值，其意表其参与意愿将与特定一阈值为代币数量送至一分叉 $r_{i1}^0 \in \mathbb{N}$ 相同；虽其为特别具体的为用户于使用介面来以一比例来测想，我们将视这些多观点为可互相替代的。

⁴⁴ 因分叉轮将不会有和一正常上诉轮具有一相同的激励机制，包含为 ETH 或 PNK 重新分配，一方可能会担心 PNK 持有者将不会提供一“完整排列阶级”。确实，如果 USR_i 提供一 $r_{ij}^0 = r_i^0$ 为所有“可接受”之选项，系统将开始来模拟一审批投票，而此为敏感对于陪审员究竟以何基准来判断何为“可接受”的 [53]。

任何质押于法庭且无一分叉偏好的 **PNK**，将不被提供于一分叉削减期间。任何非质押中的 **PNK**，且于分叉轮投票并非提交之场合，其将被传送至主分叉⁴⁵。当前一轮结果之 **PNK** 重新分配已完成于各分叉，参与分叉投票之代币将会得一惠待并使其各分叉之总数量代币将最终与原始分叉数量相同。基本上一程序从各分叉重新分配 **PNK**，至”同调” **PNK** 维持于其他分叉。然而，没用于投票之非质押 **PNK** 将不会获得此惠待；而此将激励 **PNK** 持有者来参与于一分叉投票。而其实际上为非常重要来拥有一高投票参与率于任何分叉投票来最强化 51% 攻击预防性。







现在我们将使用一程序来尝试寻找一单一最有可能与最多用户来互融之分叉⁴⁶。一方将可能执行：

- 为所有 i, j ，计算 $r_{ij} = r_{ij}^0 \cdot \text{整体代币数量}$ 。
- 所有阶级排列选项 a_{main} 维持于 a_{main} 赢出分叉之所有代币持有者 USR_i 。
- 为使 $a_j \neq a_{main}$ 的各 $a_j \in A$ 选项。
 - 使用一投票者 USR_i 的列表 L_j 来阶级排列选项 a_j 但非选项 a_{main} 。
 - 使用一 L_j 的总投票数总何。表示其以 S_j 。
- 为各选项 j ：
 - 分类用户 USR_i 利用一最大值 r_{ij} 。比较 r_{ij} 与 S_j 。如 $r_{ij} > S_j$ ，则从 L_j 移除 USR_i 。
 - 重新计算 S_j 为一 L_j 所有投票者之代币数总和。
 - 重复前两步骤直到 L_j 稳定下来。
- 接着，于可能选项 j ，选择一将最大化 S_j 且使 $L_j \neq \emptyset$ 的选项。
- 所有剩余代币持有者于 L_j 将于一 a_j 获胜之替代分叉。
- 移除代币持有者于 L_j 且选项 a_j 从一原先提交之偏好，并重复此程序直到此并不生成一 j 且 $L_j \neq \emptyset$ 。此将决定其是否还是有可能之兼容分叉。

此还是最终可能成为可接受/适当为一分叉轮投票，因最终我们将希望此分叉系统能够来使社群投票移动一极为争议决定之案例。

⁴⁵ 特别是此为不可能使代币持有者来先等待见视一市场对于不同版本之 **PNK** 做出反应后才做出决定。

⁴⁶ 请注意，于此非二元之选项情况下，其将有多种方式来转换此资讯于偏好至一组持续性的分叉。例如，一方应能尝试来最大化可能分叉之总数量，而非使用一规范之最大分叉次数。此选择也将具有其独自之取舍；例如，于最大化一单一最大分叉时，一方将可能陷入一替代分叉为几乎相同巨大之情况，而其将允许次要分叉来满足一更大比例之代币池，而此将通常为一预测来生成更高效用率之一结果。藉由选择分叉规范，一方进行决策来使其更简单进行计算，避免需要程度以上地来碎化社群，并拥有良好特性来尊重以下见视到地克隆方案存在。

	% of Total PNK	Vote	Threshold for willingness to fork to b	Destination Fork
	26%	a	NA	a
	20%	a	NA	a
	12%	b	12%	b
	11%	b	30%	b
	9%	b	40%	a
	9%	a	NA	a
	7%	b	20%	b
	6%	a	NA	a

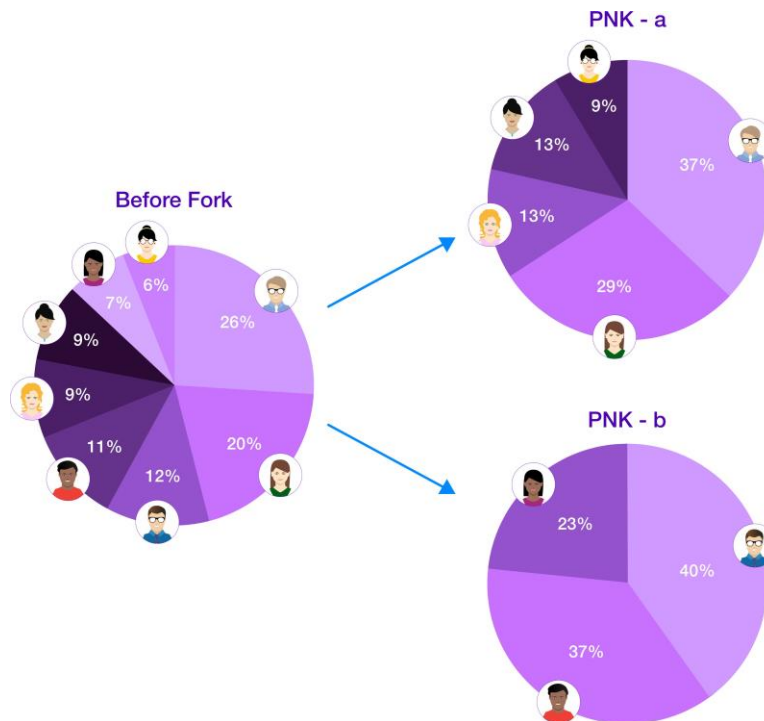


图 14: 此为 PNK 持有者之投票池于一分叉轮，此也同时表达其意愿对于进入一少数派分叉。投向选项 *a* 之 PNK 持有者也将通常表达一阈值对于其意愿来进入一少数分叉如选项确实胜出，但因 *a* 已赢出于此场合，此资讯将不会被使用且我们将会简化此部分来使图表更为简了。请注意，于一分叉轮投票至选项 *b* 之 PNK 持有者，于一包含其的分叉至 *b* 将只会此其拥有约 39% 的支持，而此将比其阈值还低，而最终将持续维持于一(主)*a* 分叉上。

4.10.2 分叉提议要素

主张 4. 以上程序将决定一可能之最大分叉

证明。我们见识到先前两循环程序使我们了解到一可能最大之代币比例来分叉至各选项 j 。而确实，一简单归纳争论显示当无一投票者被删除于第二 *for* 循环，此将可能进行延展至此分叉以任何细分情况下。于另一方面，所有投票者维延续于 L_j 于此程序后将为 $r_{ij} \leq S_j$ 当一列表被分类；因此如其同时全部转至一代替分叉，其将符合他们的选项选择。接着我们将最大化所有结果，并发现一可能的最大分叉。

第一循环将采用 $O(\#AN)$ 步骤，且 N 将会是投票者数量。分类 L_j 将花费 $O(N \log N)$ 时间。此步骤于第二 *for* 循环发生于分类之 $O(N)$ 时间后，所以整个 *for* 循环将花费 $O(N \log N)$ 时间，而重复此 $\#A$ 次，则第二 *for* 循环将需要花费 $O(\#AN \log N)$ 时间。此剩余步骤将需要其他 $O(\#AN)$ 步骤，而其整体步骤将被重复 $\#A$ 次数为一总运行时间 $O(\#A^2 N \log N)$ 。

以上步骤将被直接程式编辑至一控制分叉程序之智能合约。然而，来减低 Gas 费，此也将为可能来使用一“乐观”程序为不同可能分叉能够被提交介于时间间隔内，而智能合约将最终决定何将生成一单一最大分叉。请注意一智能合约，给予一组分叉表现为发送至代币持有者列表与一事前分类依据其分叉之每个结果，能决定其是否为有效的(同时尊重用户之表现偏好)且其是否有比目前选项分叉还宏大之分叉。

- 为使 $a_j \neq a_{main}$ 的各 $a_j \in A$ 选项。
 - 使用一于提议分叉组集合下分叉至选项 a_j 的投票者 USR_i 列表 L_j 。
 - 使用 L_j 投票者的代币总数。表示其以 S_j 。
 - 为各用户 USR_i 来验证 USR_i 并不阶级排列选项 a_{main} 且 $r_{i,a_j} \leq S_j$ 。而如果此非一情况为所有 USR_i ， a_j ，则回报“错误”。
 - 验证 S_j 为确实为单调设计，换句话说，分叉被提交依照其大小。(如 S_j 为非单调设计，回报“错误”。)
 - 开始与一最大 S_j ，查看 $S_j \geq f_j$ ，及目前分叉选择中最大分叉选择。(如果演算法呈现一 $S_j < f_j$ 价值，则回复“错误”。) 停止于 j 之第一价值，而其为 $S_j > f_j$ ，并接着回报“正确”。
 - 如演算法并非停止于 S_j 和 f_j 之比较程序，换句话说 $S_j = f_j$ 来为所有 j ，则回报“错误”
- For 循环将需要 $O(\#AN)$ 步骤，且剩余步骤将需要 $O(\#A)$ 步骤。因此，此完整运行时间为为此链上验证为 $O(\#AN)$ 步骤。

我们介绍一克隆独立性想法于分叉程序。此为启发由阶级排列投票系统中的克隆独立想法，详情请参照 [12]。

定义 1. 为一组代币持有者表达之偏好倾向，一组选项 $C = \{a_1, \dots, a_k\}$ 被宣称为一克隆选项为所有代币持有者 USR_i 。

- 无一 C 选项外只选项被阶级排列介于任何 C 内两选项。
- 要不所有选项于 C 被阶级排列，不然就是所有选项将不被阶级排列，且
- $r_{ij1} = r_{ij2}$ 为所有 $a_{j1}, a_{j2} \in C$ 。

接着，一宣称克隆独立之分叉系统，与一克隆 C 选项组集，删除考虑选项 $a_j \in C$ 将不会变更任何生成分叉为 C 组集之外之选项。(不是藉由创建此类新分叉，删除旧分叉，或变更何投票者被送至何分叉的方式)。

主张 5. 单一最大值案分叉为克隆独立情况。

证明。 请注意，为任何 a_{main} 的克隆 a' ，任何阶级排列 a' 并意涵其为可接受之投票者 USR_i ，也阶级排列 a_{main} ，所以当其将被送至主分叉，而此主分叉将不会被删除 a' 行动所影响。接着为计算多少代币愿意分叉至一选项于来使 $a_{main} \notin C$ 的克隆 $C = \{a_1, \dots, a_k\}$ 组，我们见视到 $S_{clones} = S_{j1} = S_{j2}$ 将为所有 $a_{j1}, a_{j2} \in C$ 于第二 for 循环后。除此，删除一克隆将不会变更 S_{clones} ，也其也确实不会变更 S_j 为任何 $a_j \in A$ 。请注意，如一分叉被创建当其中一 a_{j1} 赢出，则无一后续选项 $a_{j2} \in C$ 将能导致一分叉，因投票者于 a_{j2} 赢出之分叉将必须也来拥有一兼容偏好来进行至一 a_{j1} 赢出之分叉。因此，验证顺序关于何列表之 L_j 投票者进行至何分叉，除了一 C 选项组之赢出选项被 C 组以外选项替代之最常见分叉，将不会因删除一要素于 C 而受任何影响。

主张 6. 表示藉由 $T = \max_{a \in A} \{\# \text{ tokens that rank } a \text{ first}\}$ 。接着，于 WoodSIRV 投票规则下，期将会有至少 T 代币进行至主分叉。

证明。 使 a_t 成为一选项来实现最大定义之 T 。如 $a_t = a_{main}$ ，则接着 T 将至少阶级排列 a_{main} 。如 $a_t \neq a_{main}$ ，则于消除 a_t 之 WoodSIRV 步骤，将不是 a_{main} 将成为孔多塞赢家或其将比 a_t 来获取更多的首位投票于前述之重新分配步骤。不管于何情况，至少 T 数量代币必须包含阶级排列为 a_{main} 。

此主张将也将能被解释于攻击系统之成本，特别是关于多少代币必须被送至一分叉来使一恶意结果赢出于此分叉。我们见识到 WoodSIRV 为至少和二元系统具有相同等级之攻击预防性；然而，于一极端场合当个投票者将只阶级排列一单一选项且投票执案退化至二元模式，此效用结果将被有所限制。

4.11 攻击预防性

为使建立一可信赖之争议解决系统，Kleros 需要足以经受参与者中的任何可能恶意行为。于此章节，我们将详细讨论 Kleros 针对一系列高关联度之特定攻击的预防性。

4.11.1 购取半数代币攻击

如一方(或一共谋之团体)购取半数代币，其将能恐控制普通法庭并最终决定法庭之所有执案结果。然而，一方购买所有代币之情况为几乎不可能发生，特别是当代币被确实公平分配。

首先，半数代币需要为可供出售，而此情况并非随时保证。除此，一方能负担半数代币量于目前市场价格将不一定代表其确实能足以半数代币。因代币将拥有一价格增加之边际成本；而其将被时常动态地定价于所有交易所。所以如一方试图来购买一大比例额量之代币，此代币价格将迅速上升并使购买行为将花费成本越生越高。

最后，此类攻击也极有可能导致一于 4.10 章节所讨论之分叉状况。虽然分叉无法预防攻击者来成功掌握半数代币量并操纵执案结果，其能达成的为分离恶意攻击者代币与其他社群代币，并限制攻击者之代币价值且迫使其必须吞下高额损失成本。为详情关于此类预防效应，请查看图 15。

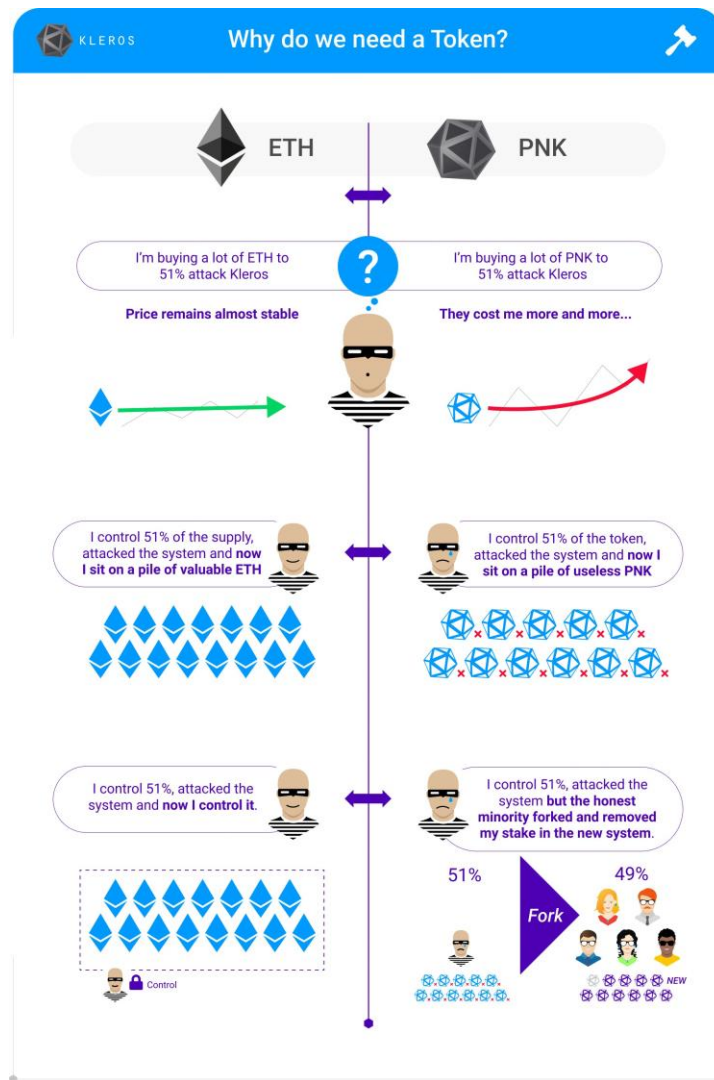


图 15: 拥有一系统代币之总结，如形容于 4.5.1 章节，关于 Kleros 之预防性对于尝试来购取半数代币之攻击

4.11.2 贿赂攻击

上诉为一重要机制来预防贿赂。贿赂一小群体之陪审员为相较来讲简单。然而，因受害者总是能有上诉之权利，攻击者可能必须要来贿赂越来越多陪审员与一急速攀高之成本。且攻击者必须来准备花费一巨额成本来贿赂一路至普通法庭，并冒着最终损失浪费全部花费成本的分险。来控制整体法庭之判决，攻击者必须来贿赂总共持有量高于 50%PNK 总量之代币持有者⁴⁷。

⁴⁷ 请注意，相似与“购买半数代币”攻击，最终一攻击的可行性将依赖于是否 50%的总代币量遭贪腐。于此，因攻击者并非自行持有代币，此可能攻击互动结果将与以上讨论之市场价格深度效应有些稍微不同。然而，于此情况，一成功攻击于普通法庭还是极有可能来大幅下降此代币之价值(因无人想要使其合约来被制裁被一非诚实法庭对吧?)。因此，一攻击者应至少准备高于 50%之预期花费成本来使其贿赂攻击成功，因价格下跌情形将预计来发生(而于几乎所有场合，攻击花费成本将远高于争议现有质押额)。

此类型攻击将不会发生于一多数诚实之模式下(当过于半数之代币由否决贿赂之诚实参与方所控制)。但即使与一非诚实多数之情况(当多数代币持有者之目标为最大化其利益)，此系统还是能于一定情况下对抗贿赂攻击。实际情况下，一方上诉所有执案决策一路至普通法庭的机率极小。然而，此机率需要存在来使激励机制来确实保持平衡。

4.11.3 $p+\epsilon$ 攻击

一 $p+\epsilon$ 攻击为一精心设计的贿赂，而其仅承诺来只有于攻击不成功时才会支付贿赂，详情请参照 [17]。此类攻击为特别设计来针对谢林游戏，尝试来玩弄其激励架构。此攻击需要一较高预算花费来发起，可一但成功，其成本将会是零⁴⁸。已于 [17]，其有一提倡之博弈做出回应针对此用户使用多方策略之类型攻击(陪审员将只会接受贿赂于一定义之机率性，而其会想尽可能预期回报而非只是单单接收贿赂)。

除此，我们已先前实施 Kleros 的”Doges 受审”试点测试实验来看看用户将于一 $p+\epsilon$ 攻击情况下如何反应。为此实验之详细结果，请参照 [29]。一方能于 [29] 评论中发现，一形容于评论 1 部分之轮-基础重新分配机制将会导致”孤独的理性之声”现象，并大幅减低 $p+\epsilon$ 攻击之可行性。

4.11.4 随意上诉攻击

当上诉机制服务为一防御来对抗贿赂攻击，其也创造其他可能性来使具有丰富资源之攻击者来攻击系统藉由持续重复上诉到一境界当其他参与方将无法继续支付上诉费用⁴⁹。我们详细解释于 4.8.2 章节，一数量之可能机制来使可被仲裁合约来激励第三方资助者来资助认为诚实之上诉方，而其使此随意上诉攻击效应有所减轻。

4.11.5 延迟忧悲

此相关攻击将成为一攻击者尝试来上诉只因其想延迟此执案审行。例如，或许攻击者为诚实方之竞争对手，且希望透过延迟诚实方接收到胜诉案例资金的时间点。不像于其他先前攻击，我们不考虑此类型攻击者欲想变更最终结果，因此我们的对应预防无法简单阻止攻击者花费上诉资金来蓄意达成其期盼之延迟结果⁵⁰。然而，再次提醒，此上诉费将随轮数增加而呈现指数性成长，而一攻击者将无法长时间来持续此类性延迟行动。除此，普通法庭具有一参数来限制一最大陪审员数，而其表示超过此数量之上诉为不可行，详情请参照 4.8.1 章节。因此，一将会有一上限为攻击者能获得之延迟时间藉由此忧悲攻击。

4.11.6 克隆忧悲

我们形容一忧悲于众筹机制，详情请参照 4.8.2 章节，于一非二元选项情况下。我们称之为忧悲”克隆资助”。想法于此为，Frederick 资助些(诚实)选项 a_j ，而其与选项 a_k 十分相似。资助 a_k 为几乎不太可能成为有利益的，因为一方能预期陪审员将执案为此两选项与一相近可能性，然而因为有需要支付至给陪审员的费用产生，Frederick 及攻击者将于此情况下参与一相同赢出机率性的负总

⁴⁸ 即表示，于一成功之 $p+\epsilon$ 情况下，攻击者将无需来支偿为任何参与者，且能恢复其所有锁赌上之资金。尽管如此，为一攻击者来锁赌一足够资金来使其他参与者确信其确实有一能力来支付所有可能贿赂将代表一机会成本因为攻击者无法使用此资金为其他目的于此同一时期。

⁴⁹ 请注意，以一纯攻击型态，此将只相关联于一当双方两侧都支付此上诉费用且胜诉方获得此费用退款之上诉费用设计架构，详情请参照 4.8 章节。

⁵⁰ 愿意接收一费用成本来同时伤害一被害者的攻击者，即表示攻击者和被害者双方将陷入一对谁都不好的环境，而此情形将被形容于”忧悲”，详情请参照 [18]。

和游戏。此忧悲情况相关联与所有考虑于 4.8.2 章节之所有众筹设计架构。于下列主张中，为不允许来利用同时资助多选项来做对冲保险之设计架构，我们将以 $r(k)$ 成为被资助之选项数量(除了被 Frederick 资助的之外)。

主张 7. 假设所有参与者拥有相同预测为各选项结果之赢出机率。而如果 Frederick 资助一选项 a ，而其预测此将有一最高之最终赢出机率。接着一策略来资助一组集之其他选项(们) K ，不包含前一轮之赢家选项 b ，所以全数考虑选项将需要一相同质押要求，并具有相同目标来减低 Frederick 的预测回报，而其有一最大忧悲要素 $\frac{1-r(k)+k}{r(k)}$ 。特别是，如 $r(k) = \frac{k+1}{2}$ ，则此忧悲要素将最大为一。而且，于 4.8.2 章节的第四设计架构，如 $r(k) = \frac{k+1}{2}$ ，则任何克隆资助策略来资助一不包含选项 b 的选项组集将具有一最大忧悲要素一。

证明。 我们使用 4.8 章节之标记符号。假设 Eve 资助选项 c_1, \dots, c_k 而各具有 $p_{c_i} \leq p_a$ ，且 $s_{c_i} = s_a = s$ 。则接着使用 $\frac{p_a + \sum_i p_{c_i}}{k+1} \geq \frac{\sum_i p_{c_i}}{k}$ 和 $\sum_i p_{c_i} \leq 1 - p_a \leq 1 - \frac{1}{1+k}$ ，我们将有

$$\begin{aligned} E[\text{Frederick}] &= p_a \left((\gamma(k) - 1)x + \sum_i s_{c_i} \right) + \left(\sum_i p_{c_i} \right) (-x - s_a) - \left(1 - p_a - \sum_i p_{c_i} \right) \frac{x}{k+1} \\ &\geq s \left(kp_a - \sum_i p_{c_i} \right) + x \left(p_a (\gamma(k) - 1) + \frac{\sum_i p_{c_i}}{k} - \frac{1}{k+1} - \sum_i p_{c_i} \right) \\ &\geq x \left[\frac{\gamma(k) - 1}{k+1} + \left(1 - \frac{1}{k+1} \right) \left(\frac{1}{k} - 1 \right) - \frac{1}{k+1} \right] = -x \frac{1 - \gamma(k) + k}{k+1}. \end{aligned}$$

相似之，使用 $p_a \geq \frac{1}{k+1}$ 我们会有

$$\begin{aligned} E[\text{Eve}] &= \left(\sum_i p_{c_i} \right) s_a + p_a \left(-\gamma(k)x - \sum_i s_{c_i} \right) - \left(1 - p_a - \sum_i p_{c_i} \right) \frac{kx}{k+1} \\ &= s \left(\sum_i p_{c_i} - kp_a \right) - \gamma(k)x p_a \leq \frac{-\gamma(k)x}{k+1}. \end{aligned}$$

请注意此界限值为锋利的当 $p_a = \frac{1}{k+1}$ 。

除此，于 4.8.2 章节的第四设计架构之下，为使 $j = 1, \dots, t$ ，而如 Eve 提供额 A_j 来资助组集 S_j 来使 $a, b \notin S_j$ 且 $p_a \geq p_c$ 为所有 $c \notin S_j$ ，接着我们将获得类似之

$$\begin{aligned}
& E[\text{Frederick}] \\
&= \sum_{S_j} \frac{A_j}{\gamma(\#S_j)x + \sum_{c \in S_j} s_c} \left(p_a \left((\gamma(\#S_j) - 1)x + \sum_{c \in S_j} s_c \right) + \left(\sum_{c \in S_j} p_c \right) (-x - s_a) + \left(1 - p_a - \sum_{c \in S_j} p_c \right) \frac{-x}{\#S_j + 1} \right) \\
&\geq \sum_{S_j} \frac{A_j}{\gamma(\#S_j)x + \sum_{c \in S_j} s_c} \left(-x \frac{1 - \gamma(\#S_j) + \#S_j}{\#S_j + 1} \right)
\end{aligned}$$

和

$$\begin{aligned}
E[\text{Eve}] &= \sum_{S_j} \frac{A_j}{\gamma(\#S_j)x + \sum_{c \in S_j} s_c} \left(\left(\sum_{c \in S_j} p_c \right) s_a + p_a \left(-\gamma(k)x - \sum_{c \in S_j} s_c \right) - \left(1 - p_a - \sum_{c \in S_j} p_c \right) \frac{kx}{k+1} \right) \\
&\leq \sum_{S_j} \frac{A_j}{\gamma(\#S_j)x + \sum_{c \in S_j} s_c} \left(\frac{-\gamma(\#S_j)x}{\#S_j + 1} \right).
\end{aligned}$$

然而，为 $r(\#S_j) = \frac{\#S_j + 1}{2}$ ，我们将有

$$\frac{1 - \gamma(\#S_j) + \#S_j}{\#S_j + 1} = \frac{\gamma(\#S_j)}{\#S_j + 1} = \frac{1}{2},$$

所以此也将生成一最大为一的忧悲要素。

特别是，我们注意到于一只有两选项被资助之设计架构下，克隆资助将具有一最大忧悲要素 1。此也能被获得于此设计架构下来允许对冲保险利用同时资助多重选项，以一更加复杂之功能函数 $r(k)$ 作为代价。

4.12 治理机制

随着 Kleros 协议增加其用户数及使用案例数，其将可能需要来添增新法庭，且来变更法庭政策及参数并定期更新及添增新功能于平台。此类型决策将会被决定由代币持有者，而其投票决定权将依据由其拥有之 **PNK** 额量。此治理机制将能被用于：

1. 设置政策：政策为指导方针关于如何解决争议。其等同于法律于传统司法系统。此将决定何方应赢出于一争议当一系列之特殊情况条件符合。此政策能特定设计为各法庭。

2. 创建新法庭。

3. 调整法庭参数，例如：

- (a) 仲裁费
- (b) 各法庭之开庭时间长
- (c) 最低代币质押量

4. 批准(或移除)一提供为应用程式之投票或激励系统替代模组，而各选择将会有不同取舍特性，详情比较请参照 4.7 章节。

5. 变更 Kleros 依赖之其中智能合约。此允许随意更改。而此也将可能被用于定期更新或紧急更新如 Kleros 系统呈现非正常运作之情况⁵¹。

Kleros 治理决议将被执行于链上如下：首先，PNK 持有者将投票于链下之 Snapshot [35]。则一列表之执行投票交易与其相对应之投票决策将与一汇款押金被提交至一治理合约。此交易列表将能被挑战；而于一挑战情况下，一方将利用 Kleros 的链外预言机数据提供能力来利用 Kleros 技术性法庭来决定提交之交易，是否确实，为相应对与投票之情况于 Snapshot。

5. 额外之未来研究

以上，我们已针对些许重点来进行讨论，而我们正致力于未来研究发展来积极改进多方面向。于此章节，我们将考虑到其他还未被讨论之些许改进方案。

5.1 重新分配机制于无一陪审员为同调之审议轮

如上述讨论，仲裁费和损失 PNK 汇款押金将被重新分配于各轮至所有与最终结果同调之陪审员。如无一陪审员于此特定审议轮，此重新分配额将被送至治理者方，而其用途将可被治理程序来所决定。

即使于一只有三陪审员之审议轮，其将成为相对来讲稀奇来看见一无陪审员同调的结果产生。然而，来使 Kleros 也能成为成本有效可能方案为非常小规模之争议，如平台内容管理，详情请参照 6 章节，其将有时也可能需要来开始与只有一最初陪审员单一投票之情况。于此案例情况下，此将有一陪审员于第一审议轮无法从其他陪审员方赢取 PNK 汇款押金(因无其他陪审员)的问题，然而尽管如此，其需要冒着损失其自身之 PNK 汇款金至治理者之风险，而此状况将导致激励机制效能被减低。于未来研究方向，我们将考虑一机制来使治理者自动重新分配从因无人能被抽选成为陪审员而使无一陪审员同调之情况下所累积之额至其相对应法庭。因此，此将平均补偿陪审员损失之汇款押金，为一其尝试诚实投票但不管如何还是会与最终执案不同调之情况。

5.2 合约隐私

为使解决争议，参与方可能会被要求来提供机密资讯至陪审员。来预防外部观察者来随意入手此机密资讯，于未来，此合约之母语语言合约(英文或其他语言)与陪审员之投票选项标记将不会被公开释放，特别是，其将不会被存入于区块链上。当合约被创建，创建者将提交一哈希(合约_文本，选项_列表，随值)(而其中合约_文本意表此合约之英文文本，选项_列表为陪审员可投票之选项列表，而随值为一随值来避免彩虹表的使用)。

合约创建者将送至此{合约_文本，选项_列表，随值}至各方使用不对称加密技术。而于此方式，参与方能验证提交之哈希确实与获得之讯息相符。于一争议发生场合，各方能揭露此{合约_文本，选项_列表，随值}给陪审员，而陪审员将能接着利用提交之哈希来进行验证。此能被达成

⁵¹审计和审查将被执行于程式部署前。然而，此将无法被 100% 保证其完全无一程式漏洞瑕疵(于程式本体或激励方面)。使其具有失败-保障将提供额外之安全性。

利用不对称加密以使只有陪审员接收至此合约本文即其选项。此以上所有步骤将被处理就由用户运行且与 Kleros 合作之應用程式。

5.3 液态投票于治理

于上述之治理章节，我们论及关于代币持有者能为平台进行一系列之决策。于此章节，我们将形容一未来计画来使代币持有者能选择来不直接进行投票并选择来指派代表投票，利用一液态投票机制 [27]。当一用户无法成功来投票，其投票权利将自动转送至其指派之投票代表。液态投票机制之简易插图将呈现于图 16。此指派投票程序也能被架构来使不同指派方为不同类型投票；例如，为投票关于不同法庭之参数议题，选项来指派至多方专家为各个法庭将被允许。请注意，指派将无需人类参与。其能成为智能合约自动导入随意复杂的投票规范(例如，投票关于费用更新将自动依照目前市场数据)。

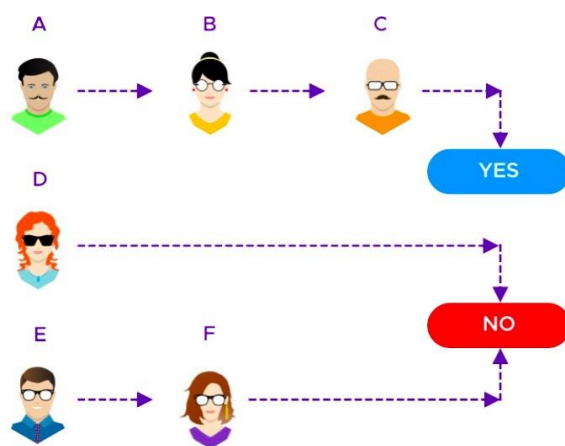


圖 16：液態投票插圖

5.4 结算逻辑

此将可能会有一情形，于一系列之上诉发生中，原先之争议上诉方们达成共识关于原先之争议额将如何被分配，且期盼提早结束此争议解决程序。我们打算添加逻辑至标准争议智能合约模组来使此可能化⁵²。

然而，介于与其他人起争议期间，例如陪审员和费用资助者，将会成为经济性感兴趣对于来使结果成为正确的。而确实，Kleros 依赖于允许第三方进行资助及调用上诉程序来保障陪审员于一些特定之攻击场合。因此，此为必要的来使争议来持续进行，即使原先争议发起双方可能已不参与于此争议内。

6 應用程式

Kleros 为一般性及多功能性之系统来被设计使用于多数情况场合。我们将于以下呈列些许可能用途之范例：

⁵² 目前版本之 Kleros 第三方托管服务只提供一限制架构为总结算情形，然而此只被提供于触发一争议前。

- **第三方托管**：来支付为一链外商品或服务，而牵涉资金将被放置于一智能合约内。于接收商品或服务后，购买者将能解锁此资金至卖家。于一争议场合，Kleros 能被使用为一仲裁智能合约决定来赔偿买家或支偿卖家。此类型 Kleros 基础之第三方托管服务已目前正进行运用中，详情请参照 [33]。

第三方托管也能被复杂多样化。例如为一租借合约，租借者可能来被要求来支付些汇款押金。而于租借财产遭损坏且租借者愿意来为此支付赔偿金，财产持有者能创建一争议来要求被支偿一部份之汇款押金。

- **微任务**：去中央化平台能来支付为微任务(类似于 Amazon Mechanical Turk 计画 [1])。任务挑战者将汇款一小额押金，并提交要求之解答来完成此任务。此任务将被重复进行。如一任务获得许多不同解答，一任务挑战者将可能会承认其其实回答错误，而其将会传送部份之汇款押金至正确回答此任务之挑战者。当于多数挑战者坚信其各自解答为正确场合时，一争议解决程序将被启用，而最终一败诉挑战者将必须传送其汇款押金至胜诉方。此系统之一范例为 **Linguo**，一去中央化翻译平台，而于此翻译之品质将可被挑战，而争议结果将由 Kleros 陪审员所决定。

The screenshot displays the Kleros Escrow web interface. At the top, there's a navigation bar with the 'ESCROW' logo, a mail icon, and a 'New Payment' button. The main content area is titled 'Payment Details' and contains the following information:

- Title:** Monero x ETH Transaction
- Receiver:** 0x7d40...B6B8c
- Escrow Type:** General
- Timeout Date and Time (Local Time):** Sun Apr 28 2019 23:30
- Amount:** 0.1 ETH
- Agreement Documents:** A document icon is shown.
- Description:** [Receiver] agrees to send [ETH] to [Monero Sender] before [28.04.2019 11:30 PM]. Once [Receiver] receives [XMR] they release funds to [Monero Sender].

Below the details, a large blue box asks: 'Did the other party fully comply with the agreement?'. It features two buttons: 'Yes' and 'No'. At the bottom, there are instructions: '1. If you select Yes, you'll pay the amount in full.' and '2. If you select No, you will be directed to a settlement screen where you can waive part of the payment to the other party or raise a dispute.' A timer indicates 'Payment times out in 0:00:05:13.'

圖 17：一 Kleros 第三方託管服務之用戶正決定是否來提起一爭議。

- **保险**：被保险者将会支付一费用至保险者来使其能获得一补偿金当某一指定之活动场合发生。保险者将可能会进行一安全汇款押金来为多方参与之被保险者(同时尊重风险管理规则)。而当一指定保险活动发生，保险者将会验证此并补偿此被保险者。如保险者不确实来验证并补偿支付为此发生之指定保险活动，一争议解决程序将开始进行。如被保险者最终胜诉于此争议解决程序，先前保险者锁上之安全汇款押金将被传送至此被保险者。于安

全汇款押金牵涉至多方被保险者且请求金额超越此锁上之此资金时，另一争议解决程序将被生成来决定此资金将如何平分于各方被保险间。

- **预言机：**一去中央化数据提供来为智能合约使用，而此用途也是以太坊早期之一重要使用案例之一 [14]。一方(其能为一智能合约)将会询问一问题，而所有其他参与方将能汇款一押金并回答此问题。如所有参与者提交相同之一解答，此解答将会回报由一预言机数据源。如其中许多相异回答产生，一争议解决程序将产生进行。预言机将回报此争议解决程序所提交之最终解答，而提交错误数据解答之参与者将会损失其汇款押金，且此损失金额将被传送至提交诚实回答的参与方。**Realitio** 提供一预言机数据服务基于此原则，而其使用 **Kleros** 当作一争议解决程序 [6]。除此，其他利用 **Realitio** 的预言机服务之应用程式，例如 **CryptoUnlocked**，[44]，也间接性地依赖此争议解决机制。其中特别是，我们已正进行研究多重方式来使此争议解决程序足以来适用来输出一真实-数字价值，例如一价格预言机的使用案例。
- **策展列表：**策展列表能同时被利用于白名单或黑名单之双方场合。例如，一白名单能列举一系列已进行正式安全审检程序之智能合约。而一黑名单能列举一系列之乱登记 **ENS** (**Ethereum Name Services**/以太坊命名服务 [2]) 名称 (例如，一恶意参与者将可能登记“**kleros-token-sale.eth**”，来尝试欺骗用户来传送资金至此帐户)。任何参与者皆能提交一物件与一安全汇款押金至此策展列表。而如果无一其他参与者于一指定时间内争议质疑该物件于此策展列表之合适性，此 **ENS** 将会被添加于此列表内且先前之汇款押金将被退款至原先资金提供主。而如果一方争议质疑此名称于此策展列表之合适性，其将汇款一安全押金，而一争议解决程序将随其产生。如最终此争议质疑物件最终被判决属于此列表内，此将被添增至表内，且物件提交者将会获得争议质疑方汇款押金。**Kleros** 已准备好来被用于代币策展列表用途，来为策展满足拥有多特性之代币 (例如，是否确实为一 **ERC20** 代币) [34]。其中一注目应用程式于 **Kleros** 为 **Proof of Humanity** (人性证明)，而其为一策展列表专门为清楚登记真实人类 [38]，而陪审员于此将必须考虑关于有所限制之人类辨识资讯 (例如面部特征) 来调解争议挑战关于不存在之伪造人类或已先前登记至此列表之重复人类。此“**Proof of Humanity**” (人性证明) 系统将提供一能预防女巫攻击之真实人类列表，而其可成为一重要应用于二次方投票系统 [41]，或为一更加有效率之空投活动等等。更一般来说，策展平台 [36]，将提供一策展列表为所有策展列表。因此，此系统将允许任何参与者来创建其独自之策展列表，且受制于全球性规范下来被包含至一顶级注册登记列表系统中。

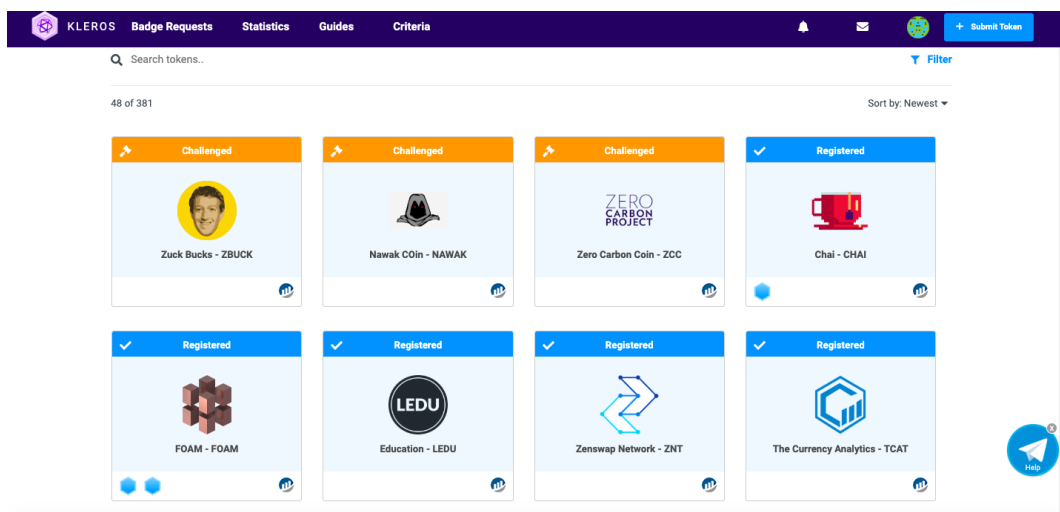


图 18：一以 Kleros 为基础之代币策展列表，其中代币地址及标章必须为确实正确来被允许纳入于此列表内

- **社交网路**：预防讯息滥发攻击，诈骗，或其他系统滥用为一重要议题为所有去中央化社交平台。参与方能回报一违规平台规范的案例与一安全汇款押金。而如果此违规为具争议性的，一争议解决程序将被启用。如此最终裁决为此回报内容并非违规，回报质疑者将损失其安全汇款押金至被质疑方。而如一违规并非被争议质疑或验证由 Kleros，多重效应将可能来被导入发生：此质疑内容被移除，内容发信者将损失参与时签署之汇款定金，且其其他内容之发信范围将被适当缩减。

7. 结论

我们介绍 Kleros，一去中央化法庭系统来使争议解决程序可行于智能合约，藉由依赖经济性激励之众招陪审员。您能鉴识一 Kleros 运行方式总结于图 19。

数位经济的起头创建一横跨国际边界的即时劳工，资本，及产品市场。此点对点经济体系需要一快速，实惠，去中央化及可信赖之仲裁机制。Kleros 使用博弈理论及区块链创建一多功能争议解决协议，而其能够来支持一大量应用程式于电子商业，金融，保险，旅游，国际贸易，消费者保护，知识产权，学术专业及其他多重领域用途。加密货币将给予许多人来首次机会来创建其银行帐户并能够安全地传送及接收资金。加密货币正帮助全球上百万人来加入金融世界。

Kleros 也将会为正义司法方面朝向同一目标来使于传统司法制度过于昂贵处理之大量合约争议能够透过 Kleros 来被公平仲裁。就如比特币实现为”无银行帐户的群众来提供银行金融服务”，Kleros 将有潜力来为所有”无法接受正义服务的群众来提供正义服务”。

参考文献

- [1] Amazon mechanical turk. <https://www.mturk.com/>.
- [2] Ethereum name service. <https://ens.domains/>.
- [3] Gnosis. <https://gnosis.pm/>.
- [4] American Bar Association. How courts work. https://www.americanbar.org/groups/public_education/resources/law_related_education_network/how_courts_work/appeals/, 2019.
- [5] Kenneth Arrow. A difficulty in the concept of social welfare. *Journal of Political Economy*, 58, 1950.
- [6] Federico Ast. Kleros-realitio oracle service - getting real information on-chain. Kleros Blog, <https://blog.kleros.io/the-kleros-realit-io-oracle/>, 2019.
- [7] Federico Ast and Bruno Deffains. When online dispute resolution meets blockchain: The birth of decentralized justice. *Stanford Journal of Blockchain Law and Policy*, 2021.
- [8] Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *SIGACT News*, 15(1):23–27, 1983.
- [9] Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch. Verifiable delay functions. In *Advances in Cryptology – CRYPTO 2018 - 38th Annual International Cryptology Conference, 2018, Proceedings, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, pages 757–788. Springer Verlag, 2018.
- [10] Dan Boneh, Manu Drijvers, and Gregory Neven. Compact Multi-signatures for Smaller Blockchains: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part II, pages 435–464. 2018.
- [11] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. *Journal of Cryptology*, 17(4):297–319, 2004.
- [12] Felix Brandt, Vincent Conitzer, Ulle Endriss, Jérôme Lang, and Ariel D. Procaccia. *Handbook of Computational Social Choice*. Cambridge University Press, New York, NY, USA, 1st edition, 2016.

- [13] Gilles Brassard, David Chaum, and Claude Cr epeau. Minimum disclosure proofs of knowledge. *J. Comput. Syst. Sci.*, 37(2):156–189, 1988.
- [14] Vitalik Buterin. Ethereum, a next-generation smart contract and decentralized application platform. <https://github.com/ethereum/wiki/wiki/White-Paper>, 2014.
- [15] Vitalik Buterin. Schellingcoin: A minimal-trust universal data feed. *Ethereum Blog*, <https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universaldata-feed/>, 2014.
- [16] Vitalik Buterin. On anti-pre-revelation games. *Ethereum Blog*, <https://blog.ethereum.org/2015/08/28/on-anti-pre-revelation-games/>, 2015.
- [17] Vitalik Buterin. The $p + \epsilon$ attack. *Ethereum Blog*, <https://blog.ethereum.org/2015/01/28/p-epsilon-attack/>, 2015.
- [18] Vitalik Buterin. The triangle of harm. https://vitalik.ca/general/2017/07/16/triangle_of_harm.html, 2017.
- [19] Vitalik Buterin. Minimal anti-collusion infrastructure. <https://ethresear.ch/t/minimalanti-collusion-infrastructure/5413>, 2019.
- [20] Benedikt B unzy, Steven Goldfeder, and Joseph Bonneau. Proofs-of-delay and randomness beacons in Ethereum. http://www.jbonneau.com/doc/BGB17-IEEESEB-proof_of_delay_ethereum.pdf, 2017.
- [21] Craig Calcaterra, Wulf A. Kaal, and Vlad Andrei. Blockchain infrastructure for measuring domain specific reputation in autonomous decentralized and anonymous systems. <https://ssrn.com/abstract=3125822>. U of St. Thomas (Minnesota) Legal Studies Research Paper No. 18-11.
- [22] Lyn Carson and Brian Martin. *Random Selection in Politics*. Praeger, 1999.
- [23] Chainlink Team. Chainlink VRF: On-chain verifiable randomness. <https://blog.chain.link/verifiable-random-functions-vrf-random-number-generation-rng-feature/>, 2020.
- [24] Alisa Cherniaeva, Ilia Shirobokov, and Omer Shlomovits. Homomorphic encryption random beacon. *IACR ePrint Archive*, <https://eprint.iacr.org/2019/1320.pdf>, 2019.
- [25] John R. Douceur. The Sybil attack. In *Revised Papers from the First International Workshop on Peer-to-Peer Systems, IPTPS ’01*, pages 251–260, London, UK, UK, 2002. Springer-Verlag.

- [26] O. Dowlen. The Political Potential of Sortition: A Study of the Random Selection of Citizens for Public Office. Luck of the draw : sortition and public policy. Imprint Academic, 2008.
- [27] Bryan Ford. Delegative democracy. <http://www.brynosaurus.com/deleg/deleg.pdf>, 2002.
- [28] David Friedman. A positive account of property rights. Social Philosophy and Policy, 11, 1994.
- [29] William George. Doges on trial curated list observations part 2 - deep dive edition. Kleros Blog, <https://blog.kleros.io/cryptoeconomic-deep-dive-doges-on-trial/>, 2018.
- [30] William George. Voting systems for multiple choice Schelling games. <https://github.com/kleros/research-docs/blob/master/multiplechoiceschelling/multiplechoiceschelling3.pdf>, 2020.
- [31] William George and Clément Lesaëge. A Smart Contract Oracle for Approximating Real-World, Real Number Values. In International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2019), volume 71 of OpenAccess Series in Informatics (OASICs), pages 6:1–6:15, Dagstuhl, Germany, 2019. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.
- [32] Allan Gibbard. Manipulation of voting schemes: A general result. Econometrica, 41(4):587–601, 1973.
- [33] Stuart James. Kleros Escrow explainer - secure your blockchain transactions today. Kleros Blog, <https://blog.kleros.io/kleros-escrow-secure-your-blockchaintransactions-today/>, 2019.
- [34] Stuart James. Kleros TCR - a deep dive explainer. Kleros Blog, <https://blog.kleros.io/kleros-ethfinex-tcr-an-explainer/>, 2019.
- [35] Stuart James. Handing over the reigns - Kleros governance moves to Snapshot. Kleros Blog, <https://blog.kleros.io/handing-over-the-reigns-kleros-governance-moves-tosnapshot/>, 2020.
- [36] Stuart James. Kleros Curate - the explainer. Kleros Blog, <https://blog.kleros.io/kleroscurate-the-explainer/>, 2020.
- [37] Stuart James. Linguo - the first decentralized translation platform. Kleros Blog, <https://blog.kleros.io/linguo-decentralized-translation-platform/>, 2020.
- [38] Stuart James. Proof of Humanity - an explainer. Kleros Blog, <https://blog.kleros.io/proofof-humanity-an-explainer/>, 2021.
- [39] Kleros Community. General court policy. <https://court.kleros.io/courts>, 2021. Consulted, June 2021.

- [40] Georgios Konstantopoulos. How does Optimism's rollup really work? Paradigm Research, <https://research.paradigm.xyz/optimism>, 2021.
- [41] Steven P. Lalley and E. Glen Weyl. Quadratic Voting: How Mechanism Design Can Radicalize Democracy. *AEA Papers and Proceedings*, 108:33–37, 2018.
- [42] L. Laudan. *Truth, Error, and Criminal Law: An Essay in Legal Epistemology*. Cambridge Studies in Philosophy and Law. Cambridge University Press, 2006.
- [43] Clément Lesaëge. ERC 792: Arbitration standard. <https://github.com/ethereum/EIPs/issues/792>, 2017.
- [44] Patrick Long. Cryptounlocked oracle upgrade. <https://blog.wetrust.io/cryptounlocked-oracle-upgrade-5c8b22e3375b>, 2019.
- [45] P. H. Madore. Augur House elections market: Alleged reporter says Republicans won the market. <https://www.ccn.com/augur-house-elections-market-alleged-reporter-says-republicans-won-the-market/>, 2018. 56
- [46] Andrew Mao, Ariel D. Procaccia, and Yiling Chen. Better human computation through principled voting. In *AAAI*, 2013.
- [47] Offchain Labs Team. Chainlink oracles now live on the Arbitrum rollup testnet. <https://offchain.medium.com/chainlink-oracles-now-live-on-the-arbitrum-rolluptestnet-59b7e5d9fed6>, 2021.
- [48] Torben Pryds Pedersen. A threshold cryptosystem without a trusted party. In *Advances in Cryptology — EUROCRYPT '91*, pages 522–526, Berlin, Heidelberg, 1991. Springer Berlin Heidelberg.
- [49] Jack Peterson and Joseph Krug. Augur: a decentralized, open-source platform for prediction markets. <http://bravenewcoin.com/assets/Whitepapers/Augur-A-DecentralizedOpen-Source-Platform-for-Prediction-Markets.pdf>, 2015.
- [50] Jimmy Rago. Using Kleros arbitration for dapps on xDai. <https://kleros.gitbook.io/docs/integrations/scalability-and-crosschain/xdai>, 2021. Consulted, June 2021.
- [51] Christian Reitwiessner. From smart contracts to courts with not so smart judges. *Ethereum Blog*, <https://blog.ethereum.org/2016/02/17/smart-contracts-courts-notsmart-judges/>, 2016.

- [52] Rachel Rothwell. The rise of global litigation funding. <https://www.raconteur.net/riskmanagement/the-rise-of-global-litigation-funding>, 2017.
- [53] Donald G. Saari and Jill van Newenhizen. Is approval voting an ‘unmitigated evil’?: A response to Brams, Fishburn, and Merrill. *Public Choice*, 59(2):133–147, 1988.
- [54] Mark Allen Satterthwaite. Strategy-proofness and Arrow’s conditions: Existence and correspondence theorems for voting procedures and social welfare functions. *Journal of Economic Theory*, 10(2):187–217, 1975.
- [55] T. C. Schelling. *The strategy of conflict*. Oxford University Press, 1960.
- [56] Markus Schulze. A new monotonic, clone-independent, reversal symmetric, and 孔多塞 consistent single-winner election method. *Social Choice and Welfare*, 36(2):267–303, 2011. [57] Shutter Network Team. Introducing Shutter Network — combating frontrunning and malicious MEV using threshold cryptography. <https://shutter.ghost.io/introducing-shutternetwork-combating-frontrunning-and-malicious-mev-using-threshold-cryptography/>, 2021.
- [58] P. Stone. *The Luck of the Draw: The Role of Lotteries in Decision Making*. Oxford University Press, 2011.
- [59] Paul Sztorc. Truthcoin, peer-to-peer oracle system and prediction marketplace. <http://www.truthcoin.info/papers/truthcoin-whitepaper.pdf>, 2015.
- [60] T.N. Tideman. Independence of clones as a criterion for voting rules. *Social Choice and Welfare*, 4, 1987.
- [61] Sam Vitello, Clément Lesaege, and Enrique Piqueras. ERC 1497: Evidence standard. <https://github.com/ethereum/EIPs/issues/1497>, 2018.

A 主张 1 证明

证明。表示 L 为选项数量。表示 F 为应被此审议轮中被陪审员平分之仲裁费。为一赢出选项 w 及由其他此轮投票者投下之投票选项集，其将被表示为

$$K = \sum_{USR_k \neq USR} \sum_{a_j \neq w} \mathbf{1}_{USR_k: a_j < w}$$

此为对于除 USR 之外且与最终赢出选项同调之用户的成对投票总数。相似之，表示其由

$$K' = \sum_{USR_k \neq USR} \sum_{a_j \neq w} \mathbf{1}_{USR_k: a_j \geq w}$$

此为对于除 USR 之外与最终赢出选项不同调之用户的成对投票总数。基于我们的假设，此最终赢出选项，及其他陪审员于此轮之投票，将能被考虑为固定的关联尊重至 USR 的投票。因此， K 和 K' 也同时为固定的。

请注意，此考虑之支偿函数为，提供一平局投票将不会生成一比对应严谨投票来解决此平局还多之利益。因此提供平局投票为一(虚弱)之主导策略。接着假设 USR 放置一最终胜出选项于 i 位置。接着当 USR 之投票为严谨且特别是其投票者并非放置任何其他与 w 平局之投票选项，则其将为正确为 $L - 1 - (i - 1) = L - i$ 配对且非正确为 $i - 1$ 配对。因此，当 $B = 0$ 时，其净支偿对于损失汇款押金将会是：

$$\text{payoff}(i) = \left([K' + (i - 1)] \frac{D}{L} + F \right) \frac{L - i}{K + L - i} - (i - 1) \frac{D}{L}.$$

特别是，当其支偿为一函数只有对于 i (显然非此情况当 $B \neq 0$)。请注意，此渐增 i 将导致 USR 来损失一额外汇款押金 $\frac{D}{L}$ ，而其将会被平分于其和其他陪审员间基于其同调程度。因此， USR 只能回复一部份之损失汇款押金透过其奖赏，言之

$$\text{payoff}(i) \geq \text{payoff}(i + 1).$$

接着，为任何其他投票者于此投票轮之投票组集，一标准争论显示

$$\begin{aligned}
E[\text{vote } a_1 > a_2 > \dots > a_L] &= \sum_{j=1}^L \text{payoff}(j) \text{prob}(a_j \text{ wins}) \\
&= \sum_{j=1}^{L-1} \text{prob}(a_j \text{ wins}) \text{payoff}(j) - \text{payoff}(L) (1 - \text{prob}(a_L \text{ wins})) + \text{payoff}(L) \\
&= \text{payoff}(L) + \sum_{j=1}^{L-1} \text{prob}(a_j \text{ wins}) (\text{payoff}(j) - \text{payoff}(L)) \\
&= \text{payoff}(L) + \sum_{j=1}^{L-1} \text{prob}(a_j \text{ wins}) \sum_{i=j}^{L-1} [\text{payoff}(i) - \text{payoff}(i+1)] \\
&= \text{payoff}(L) + \sum_{i=1}^{L-1} \left([\text{payoff}(i) - \text{payoff}(i+1)] \sum_{j=1}^i \text{prob}(a_j \text{ wins}) \right).
\end{aligned}$$

为最大化藉由最大化 $\sum_{j=1}^i \text{prob}(a_j \text{ wins})$ ，且因此藉由顺序排列投票选项 a_i 依照其赢出机率。当其为正确为任何任何投票者之投票组集，且此投票为独立不受影响自 *USR* 之投票及最终结果，我们将有一想要期盼之结果。

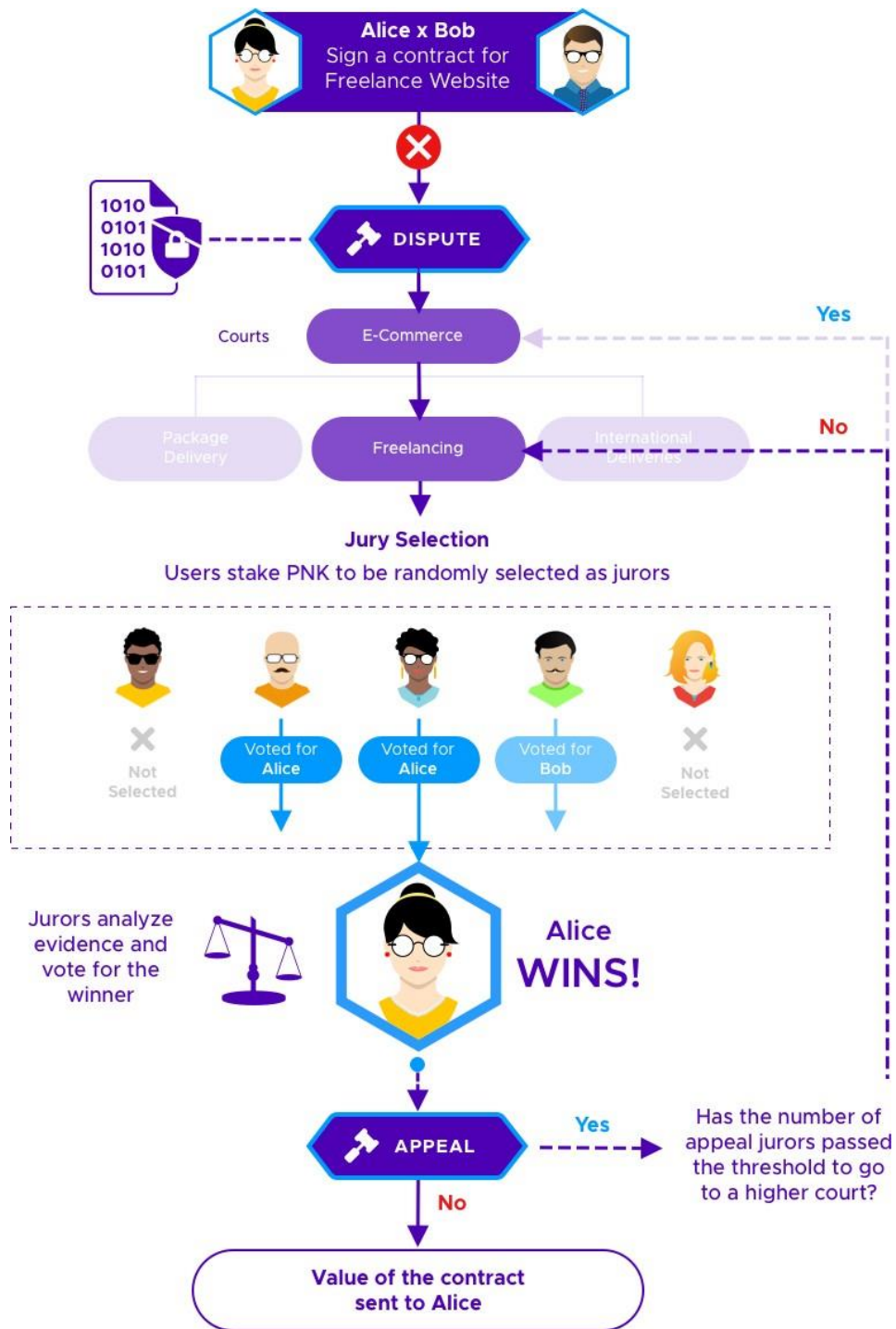


图 19：Kleros 运作之争议范例

图和方程式解析/Figures & Equations

I. 解析图用词

图 1

The majority votes: 多数投票至

You vote: 您投票至

Yes: 是

No: 否

图 2: screenshot image.

图 3

Arbitrable Side: 可被仲裁方

Users who are parties to the dispute participante here.: 争议双方将参与于此。

Curated List: 策展列表

Escrow: 第三方托管

Oracle:Oracle 预言机数据提供

Decision: 决议

Cases: 案例

Kleros Court:Kleros 法庭

Arbitrator Side: 仲裁方

Users who are jurors to disputes participate here.: 争议陪审员将参与于此。

图 4

Atomic Communication Possible: 原跨链沟通可能

Arbitrable Side: 可被仲裁方

Block state of contract pending dispute resolution by placing deposit: 藉由汇款押金，合约之区块将处于争议解决等待状态。

Result reported directly from arbitrator contract: 结果将直接报告从仲裁者合约

Arbitrator Side: 仲裁方

Deposit transferred from arbitrable side to pay arbitration fees, dispute raised: 传送汇款押金来使可被仲裁方支付仲裁费用。

Atomic Communication Not Possible: 原跨链沟通不可能

Arbitrable Side: 可被仲裁方

Bloch state of contract pending dispute resolution by placing bounty for party that raises dispute: 藉由争议发起方放置赏金来使合约状态处于争议解决等待状态。

Report results with deposit.: 报告结果藉由汇款押金

This result can be challenged, in which case wait for definitive ruling from arbitrator side to compare: 此结果将能被挑战，而此场合必须等待仲裁方之最终执案审议结果来比较。

Arbitrator Side: 仲裁方

Arbitrator Side: 支付仲裁费来发起争议。

Kleros Court: Kleros 法庭

Escrow: 第三方托管

Curated Lists: 策展列表

Oracle: 预言机

图 5

General Court: 一般法庭

Chief's Path: Chief 的途径

Clément's Path: Clément 的途径

Blockchain: 区块链法庭

Tehcnical: 技术性法庭

Non-Technical: 非技术性法庭

Token Listing: 代币上列法庭

Marketing Services: 市场营销法庭

English Language: 英文语言法庭

Onboarding: 新手报到法庭

Curation: 策展列表法庭

Curation (Medium): 策展列表(中等)法庭

Data Analysis: 数据分析法庭

Statistical Modeling: 统计建模法庭

Video Production: 影片制造法庭

Corte General en Espanol: 西班牙语一般法庭

Humanity Court: 人性法庭

图 6

Token Owner: 代币持有者

Staked: 质押

Start: 开始

End: 结束

Weight: 权重

图 7: screenshot image.

图 8

Honest1: give Bob 7 more days, 诚实选项 1: 给 Bob 多七天时间

Honest2: give Bob 8 more days, 诚实选项 2: 给 Bob 多八天时间

Dishonest: just refund Alice, 不诚实选项: 就退费给 Alice

Honest3: give Bob 9 more days, 诚实选项 3: 给 Bob 多九天时间

图 Voting System

Plurality: 复数决系统

Borda: 博达系统

Instant-Runoff: 立即径流系统

WoodSIRV: WoodSIRV 系统

RankedPairs: 阶级配对系统

Schulze: 舒尔茨系统

Clone Independent: 克隆独立性

Complexity/Gas: 复杂性/Gas 费

Condorcet: 孔多塞

Monotonic: 单调

Attack Resistance: 攻击抵抗性

No: 否

Yes as voting system: 是，为一投票系统

Bias in incentive system: 偏见于激励系统

No known bias in incentives: 无已知偏见于激励系统

Low: 低

Medium: 中

High: 高

Bad: 恶劣

Not great: 不佳

Better?: 更佳?

图 Weight Function

Weight function: 权重函数

Winner First Max Payout: 赢家首先最大支偿

Unanimous No Weight: 一致无权重

Concentration on Close Pairs: 集中于相近配对组

Yes: 是

No: 否

Intermediate: 中阶

Better: 更佳

图 9: translation not needed.

图 10

Transfer 0.2 ETH for Arbitration Fees: 传送 0.2 ETH 为仲裁费

Transfer 200 PNK for Token Redistribution: 传送 200 PNK 为代币重新分配

图 11

Expected Return: 预期回报

Honest Strategy: 诚实策略

Lazy Strategy: 懒惰策略

图 12

Jurors (Total): 陪审员 (总数)

If: 如

Wins: 赢出

If another option: 如另一选项

Paid: 支偿

Loses: 输掉

Gets back stake: 取回质押

图 13: translation not needed.

图 14

% of Total PNK: PNK 总数%

Vote: 投票

Threshold for willingness to fork to b: 意愿阈值来分叉至 b

Destination Fork: 目标分叉

Before Fork: 分叉前

图 15

Why do we need a Token?: 为何我们需要一代币?

I am buying a lot of ETH to 51% attack Kleros: 我正购入许多 ETH 来针对 Kleros 进行一 51%攻击

I am buying a lot of PNK to 51% attack Kleros: 我正购入许多 PNK 来针对 Kleros 进行一 51%攻击

Price remains stable: 价格保持稳定

They cost me more and more: 此将花费越来越多金额成本

I control 51% of the supply, attacked the system and now I sit on a pile of valuable ETH: 我控制 51%代币总量，攻击系统，然后现在我还是拥有一堆高价值 ETH

I control 51% of the supply, attacked the system and now I sit on a pile of useless PNK: 我控制 51%代币总量，攻击系统，然后现在我只剩下一堆零价值的 PNK

I control 51%, attacked the system and now I control it: 我针对系统进行一 51%攻击，而现在我控制此

I control 51%, attacked the system but the honest minority forked and removed my stake in the new system: 我针对系统进行一 51%攻击，而现在诚实少数派决定进行分叉并将我的代币移除于系统

Control: 控制

Fork: 分叉

Figure16

Yes: 是

No: 否

图 17: screenshot image.

图 18: screenshot image.

图 19

Sign a contract for Freelance Website: 签署一合约为自由职业网站

Dispute: 争议

Courts: 法庭

E-commerce: 电子商业

Freelancing: 自由职业

Yes: 是

No: 否

Jury Selection: 陪审员选择

Users stake PNK to be randomly selected as jurors: 用户质押 PNK 来被随机抽选为陪审员

Voted for Alice: 投票为 Alice

Voted for Bob: 投票为 Bob

Not Selected: 没被选择

Jurors analyze evidence and vote for the winner: 陪审员分析证据并为赢家投票

Alice WINS: Alice 获胜

Appeal: 上诉

Has the number of appeal jurors pass the threshold to go to a higher court?: 上诉陪审员数量是否已达至高阶法庭上诉要求阈值?

Yes: 是

No: 否

Value of the contract sent to Alice: 合约送至 Alice 之价值额量

II. 解析方程式用词

min_stake: 最低_质押

weight: 权重

ETH fees and lost deposits: ETH 费用及损失之汇款押金

jurors that vote for w: 为 w 投票之陪审员

options ranked above (or equal to)w: 选项阶级排列高于(或等于)w

total options-1: 总选项-1

voted: 投票向

ETH fees:ETH 费用

margin of [A] against [B]: [A]对于[B]的边缘值

total number of votes: 总投票数

prob: 机率

[A] does not put w last: [A]并非将 w 放置最后

[A] puts w last: [A]将 w 放置最后

honest: 诚实

lazy: 懒惰

number of jurors: 陪审员数量

in previous round: 于前一轮中

threshold: 阈值

previous round result or more extreme: 前一轮结果或更加极端结果

average juror would vote current winning choice first with [A] probability: 平均陪审员将会优先投票目前赢出选项与[A]机率性

Amount funded for S: 为 S 资助之额量

Return under prev. model if S has been funded alone: 退还于先前.模式如 S 被单独资助

Amount funded by [A] for [B]: 由[A]资助为[B]之额量

crowdfunder: 众筹者

remove [A] from S: 从 S 中移除[A]

against: 对

a versus singleton: a 对单例

a if opposition unfunded: a 如对抗方无被资助

utility: 效用

fct: 功能

case outcome for the fork: 分叉之案例结果

percentage of tokens that are on the same fork as me after the case: 于案例后，将与我于相同分叉之代币百分比

Frederick: Frederick

Eve: Eve

payoff: 支償

wins: 贏出

*[A][B] are random suitable words for the sentence. *