Kleros

简版 v1.0.5

Clement Lesaege and Federico Ast

2018年1月

简述

Kleros是一个建立在以太坊之上的去中心化应用，作为一个去中心化的第三方来仲裁各种从简单到复杂的合同争议。 这一争议解决系统依靠博弈论激励来让陪审员正确地进行决策， 以此获得快速，经济，可靠和去中心化的最终裁决。

1. 项目背景介绍

亚里士多德曾经说过：“谁控制法庭，就控制国家”。

当今世界正在经历的加速全球化和数字化，产生了跨管辖权用户之间的在线交易数量呈指数级增长。如果区块链技术落地普及化，在不久的将来，大多数的商品，劳动力和资本将通过去中心化的全球平台进行分配，随之而来的纠纷必定产生。比如：

- 去中心化的在线零售平台的用户会声称卖家没有按照协议规定发送货物；
- 去中心化的在线客房预定平台中的客人会声称预定的房子没有“如图所示”；
- 众筹平台中的支持者要求团队因未能兑现开发承诺而退还投资。。。等等。

智能合约具有按照程序自动执行的特性，但不能提供主观判断或考虑区块链以外的因素。现有的争端解决方式对于实时运作的去中心化全球经济而言太慢，太昂贵且

太不可靠。因而需要一个快速，经济，透明且可靠的去中心化争议解决机制，对智能合约的可执行性进行最终裁决。

于是Kleros作为一个能够解决各种争议的多用途裁决系统协议诞生了。它是基于以太坊去中心化自治组织技术（DAO），作为一个去中心化的第三方来仲裁各种从简单到复杂的合同争议。仲裁程序的每一步（获取证据，选择陪审员等）都是完全自动化的。Kleros并不依赖少数人的裁决，而是采用了博弈论的经济激励。Kleros的理论依据是现代法律认识论：法院是一种认知引擎，是一种从混乱的线索中发现事件真相的工具，它定义了代理人（陪审团）遵循使用输入（证据）产生输出（决定）（参考文献 15）的程序。

Kleros通过众包方式，区块链技术和博弈论来开发一个以安全和经济的方式产生正确决策的司法系统。

2. 早期理论：谢林币原理

谢林点（英语：Schelling point，又译为**薛林点**，或称为**聚焦点**），是博弈论中人们在没有沟通的情况下的选择倾向，做出这一选择可能因为它看起来自然、特别、或者与选择者有关。谢林用下面的例子说明了这个概念：

> ”明天你必须在纽约见一个陌生人。你在哪里和什么时候见到他？“
> 虽然在城市的任何地点和时间都可以成为解决方案，但最常见的答案是：“中午在中央车站信息亭”。

并没有什么能让中午的中央车站成为一个几率更高的地方（只要人们进行沟通协调，其他任何地点和时间都会几率均等），但它作为会面场所的传统使其成为一个自然的焦点。谢林点通常出现在沟通不可能的时候，或者缺乏信任的沟通过程（参考文献 14）。

基于谢林点的概念，以太坊创始人Vitalik Buterin提出了谢林币（参考文献 8）的概念，一种对说明真相给予经济激励的令牌。

假如我们想知道今天上午巴黎是否下雨，我们问每一位谢林硬币的持有者：“今天早上巴黎下雨了吗？是或否”。每个令牌持有人进行无记名投票，并在所有投票结果都显示出来之后，多数票的参与者将获得10%的令牌奖励，而少数票的参与者将失去了10%的令牌。

托马斯谢林（Thomas Schelling，参考文献 18）这样描述谢林点原理：“每个人期望的聚焦点是他人期望他本人期望被期望做出的选择”。谢林币使用这个原则为许多相互不认识或相互缺乏信任的参与者说出真相提供了激励。参与者投票给真正的答案，因为他们希望别人投票选出真正的答案，并且他们期望别人与自己一样投票选出真正的答案。。。在这个简单的例子中，谢林点是就是真相点。
谢林币机制已被应用在分布式预测系统和市场分析中（参考文献 19，16，3）。其最基本的一项内容就是，使每个参与者作出与其他人一致的诚实裁决是需要激励机制的。Kleros采用的激励机制就是基于谢林币机制，进行了改进以使其具有扩展性，针对性和保护隐私等特性，进而规范化裁决程序。

你的选择 / 多数选择	是	否
是	+0.1	-0.1
否	-0.1	+0.1

图1:基本谢林理论激励机制收益分配

3. 应用实例

居住在法国的企业家爱丽丝，通过点对点自由职业平台聘请了来自危地马拉的程序员鲍勃为她的公司建立一个新网站。在他们就价格，条款和条件达成一致之后，鲍勃开始工作。几个星期后，他交付了产品。但爱丽丝不满意，她认为鲍勃的工作质量远低于预期。鲍勃回复说他的产品完全符合协议中的内容。爱丽丝会感觉很沮丧，因为她不能因为几千元的合同去聘请一名律师与住在地球另一端的鲍勃打官司。

假如合同有一个条款说明：如果发生争议，将交由Kleros法院裁决。 情况会是怎样？在鲍勃停止回复她的电子邮件之后，艾丽丝点击一个“发送给Kleros”的按钮，并填写一份简单的表格来解释她的说法。数千英里外，在内罗毕，齐夫是一名软件开发人员。他在上班途中的公车“无聊时间”期间，正在检查Kleros网站以查找一些仲裁工作。他在业余时间担任自由职业者与客户之间软件开发纠纷的陪审员，可以一年赚取几千美元。他通常在网站质量子厅中裁决案件。该子厅需要具备html，javascript和网页设计知识来裁决自由职业者与其客户之间的争议。齐夫投入2PNK参与陪审员选取，Kleros使用pinakoin（PNK）来进行陪审员的随机抽取。他投入的令牌越多，他就越有可能被选为陪审员。

大约一个小时后，齐夫收到一封电子邮件：“您被选为网站质量裁决的评委。点击这里下载证据。你有三天时间来提交你的裁决“。与此同时，来自库斯科的博尼图和罗马尼亚的亚历山大都通过投入PNK参加陪审员抽取，被抽中而收到了类似电子邮件。互不相识的他们是从近3000名候选人中随机抽取而来，将协作解决艾丽丝和鲍勃之间的争议。

在回家的公交车上，齐夫分析证据并裁决谁是对的。两天后，三个陪审员投票结束，爱丽丝和鲍勃同时收到一封电子邮件：“陪审团已经裁定爱丽丝胜诉：该网站未按照双方同意的条款和条件交付。智能合约已经把钱转给了爱丽丝“。

陪审员因其工作而获得奖励之后，纠纷裁决完成。

4. 项目介绍

4.1. 裁决合约

Kleros是可选裁决方案之一。智能合约在选定Kleros为仲裁方案之时， 需要选择争议裁决需要多少陪审员以及在哪个子厅进行（参见4.8 仲裁庭分支），原则是选择一个与合约匹配专业的子厅。比如软件开发智能合约将选择软件开发子厅，一份保险智能合约将选择一家保险子厅等等。图2显示了一个用户可以选择的子厅分支示例。 Kleros团队正在制定一系列标准智能合约，作为使用Kleros作为纠纷解决方案基本子厅。

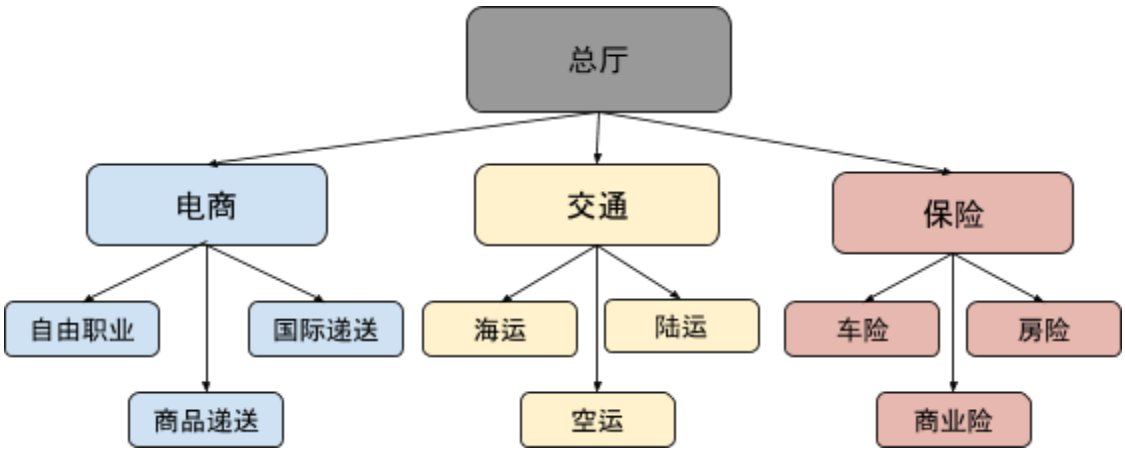


图2: 智能合约可选的子厅分支示例

4.1.1. 陪审员选项：

合同将提供陪审员投票的选项。

在上文的实例3中，选项将会是：

“退款给爱丽丝”，“多给鲍勃一周完成网站” 和 “支付鲍勃”。

裁决结束后，智能合同将执行规定的合同的行为。 在这个例子中：

- “退款给爱丽丝” - 付款退还给爱丽丝的地址
- “多给鲍勃一周完成网站” - 锁定争议并于一周后除去该选项
- “支付鲍勃” - 付款支付给鲍勃的地址

4.1.2. 隐私保护：

解决争议时有可能需要当事人向陪审员披露其私有信息，为了保护此类信息，自然语言形式的合同（英文或其他方式）以及陪审员投票选项的标签不会放在区块链上。当创建合同时，创建者提交通过哈希256加密的合同文本，选项列表和盐（合同文本是合同的简明英文文本，选项列表是陪审员可选投票选项的标签，盐是随机数以避免使用彩虹表破解）。

合约创建者使用非对称加密向每一方发送 {合同文本，选项列表，盐} 之后，各方可以验证提交的哈希与发送给他们的内容相对应。如果有争议，每一方都可以向陪审员透露与提交的哈希相对应的{合同文本，选项列表，盐}，通过非对称加密，他们可以确保只有陪审员收到合同文本和选项。所有这些步骤都由采用Kleros协议的用户端应用程序完成。

4.2. 陪审员抽取

4.2.1. 系统令牌：Pinakion（PNK）

Kleros通过名为Pinakion（PNK）的令牌为陪审员提供经济激励，它也作为持有者自愿参与陪审员抽取的依据。Pinakion（PNK）这个名字来源于每个雅典公民用作身份证明的铜牌， 当时被普遍用来作为陪审团的选择标志。 Kleros的大多数Pinakion将通过令牌分发进行分配， 少部分将给予项目贡献者和早期支持者。PNK的持有者自愿存入PNK参加陪审员抽取，并且在参与裁决后获得仲裁费用，并且获得所有存入PNK的重新分配。

被抽中作为特定争议陪审员的可能性与持有者存入参与该特定争议所在子厅的令牌数量成正比。 他存入的令牌数量越多，被抽选为陪审员的可

能性就越高。 没有存入令牌的持有者也就没有被抽中的机会，这可以防止在陪审员抽取过程中有不活跃的持有者被选中。

Pinakion在Kleros设计中扮演着两个关键的功能：

首先，它保护系统免受女巫攻击（sybil attack）参见12。 如果陪审团只是简单随机抽取的，那么恶意的当事人可能会在每次争议中创建大量的地址并被高机率抽取，从而控制裁决结果。

其次，它作为裁决激励：做出错误裁决的陪审员将损失一部分他存入的令牌，分配给做出正确裁决陪审员作为激励。

4.2.2. 选择陪审员

令牌持有人自选特定子厅并存放PNK后，智能合约随机进行陪审员的最终选择。 他被选中为陪审员的可能性与存入令牌的数量成正比。 从理论上讲，一个候选人可能会因为特定的争议而被抽签一次以上（但实际上不大可能）。 他被抽中的次数（称为权重）决定了他将在争议中获得的选票数量以及在令牌激励分配期间的获得令牌比率。

比如，6个令牌所有者参加了陪审员抽取并总共存入10,000个PNK，分配如下：

Token Owner	Activated	Start	End	Weight
A	1000	0	999	0
B	1500	1000	2499	1
C	500	2500	2999	1
D	3000	3000	5999	2
E	1500	6000	7499	0
F	2500	7500	9999	1

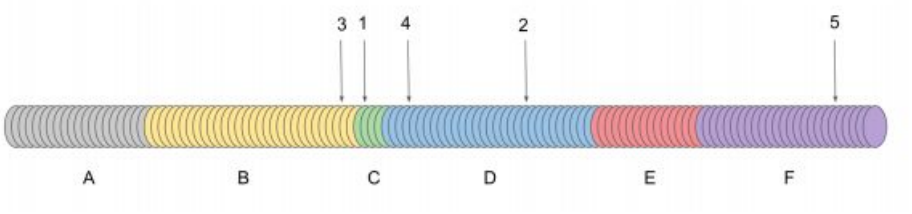


图3: 令牌存入和陪审员抽取示例

对于需要5票的争议，将从被存入的10,000个中抽出5个令牌。 比如如图3所示，假如令牌编号2519,4953,2264,3342和9531被抽中，令牌所有者B，C和F将以1的权重投票，令牌所有者D以2的权重投票。所有存入的PNK令牌在裁决决定后退回，只是投票给错误结果的陪审员那部分将被重新分配给投票给正确结果的陪审员。

4.2.3. 随机选取原理

为了防止随机选取陪审员被操控，我们需要一个过程来抽取不易操控的随机数字。 使用固定算法在两点之间选择一个随机数并不科学，因为攻击者可以用自己的多个地址制造虚拟争议，然后多次选择自己的地址担任陪审员，并选择另一名受害陪审员。 之后，他会操控自己多个地址的选票，以便从受害陪审员处窃取激励令牌（请参阅奖励系统一节）。
随机数字通过连续工作证明（PoW）（参见10）生成，通过使用类似于Buenzy等人的方案（参见11），以便使这也适用于PoS区块链（在PoW区块链中，块哈希值极难预测，正好可用作种子）。

1.初始化：

我们从seed = blockhash开始，让所有参与者输入一个本地产生的随机数localRandom来改变种子，例如seed = hash（seed，localRandom）。这样每个参与方都可以改变种子，但不选择它，因为加密哈希函数使得攻击者确定localRandom并破解（seed，localRandom）= seedAttack很困难。

2.计算主随机值：

在随机数中有利害关系的每个参与方运行种子的连续工作证明。从h0 = seed开始，他们计算h_{n+1} = hash（h_n）一直到 h_d，其中d是难度参数。计算h_d需要时间，这确保某人在获得种子并获得结果之间经过了一段时间。难度d是固定的，因此在初始化阶段期间没有硬

件可以计算h_d。因为在开始下一步之前我们需要上一步的结果，所以这个过程不能并行化。这意味着任何一方都不可能具有明显优势。

3.在区块链上获取结果：

每个参与方都可以通过令牌发布h_d， 然后其他各方可以通过交互式验证来清除错误的结果（参见17）。 它包含了对攻击者的二分搜索。

如果攻击者提交虚假h_d，验证房间可以向他询问他的h_d/ 2值，如果他给出了错误的值，那么攻击者的h0和h_d/ 2之间的值有错误。如果他给出正确的值，那么h_d/和hd之间会有错误。 无论哪种方式，搜索空间一分为二。 验证方在缩小的空间（错误发生地点）之前继续这个过程，直到剩下两个值。 然后，验证方可以在攻击者答案中展示x使得h_{x+1}≠hash（h_x），从而使该答案无效的当事人失去了令牌。 其中一部分被烧毁，另一部分给予使其无效的一方。 请注意，使错误结果无效所需的交互次数仅为O（log（d））。

4.获取所有随机值：

在所有参与方确认全部无效结果后，只剩下正确的h_d。 从这些正确结果中我们得出主随机值r_n = hash（h_d，n）。

只要至少有一个非恶意参与者，这个过程就可以产生一个随机数。 计算顺序工作证明（PoW）和交互式验证需要时间。 但是对于大多数纠纷来说等待几个小时进行陪审员抽签并不是问题。 然而，对于一些对时间有要求的次级厅来说（例如，解决区块链纠纷的子厅），这种随机数字生成方法可能太慢。 这些子厅可以使用随机数生成器，虽然相对来说安全性底但是速度更快。 有关此过程的更多详细信息以后会陆续发布。

4.3. 投票

陪审员审查证据后提交裁决选项，并同时提交哈希（裁决，盐，地址）。盐是本地产生的随机数，用来加密以防止彩虹表攻击。地址是陪审员的以太网地址，需要这个以确认陪审员身份。投票结束后，陪审员们提供各自的「裁决，盐」，Kleros的智能合约会确认他们的身份和投票。无法提供「裁决，盐」的陪审员将损失部分参与令牌（详见激励系统部分）。

在一个陪审员提交裁决后，他不允许修改。而且对于其他陪审员或当事人来说，他的裁决仍然是不可见的。这可以防止他的投票影响其他陪审员的投票。
一个陪审员虽然可以对外公布他的投票结果，但他无法为其他陪审员提供理由认为他所说的话是真实的。这就是谢林点原理的重要特征。否则的话，假如一个陪审员知道其他多数陪审员的投票，他就会投票赞成多数而不是投票给谢林点。在投票结束之前，任何展示其投票结果证据的陪审员将被剥夺参与令牌，投票将被确定为无效。

如果一个陪审员想要向另一方透露投票结果，他有两种选择：

1.透露其投票：

他无法证明自己确实投票该选项，他可能会说谎而另一方无法验证。

2.透露其投票及其证据：

他需提供投票的证据，但他也将可能因此被剥夺他的参与PNK。

这样就防止了陪审员在投票结束前透露其裁决选项。

陪审员也需要为他们的投票提供理由。在所有陪审员投票后（或在投票时间结束后），所有陪审员公开自己的投票裁决。陪审员未能透露他们的投票将损失参与令牌。最后，投票汇总并执行智能合约。具有最高票数的裁决选项被定为获胜裁决选项。

4.4. 仲裁费用

为了对陪审员的工作进行激励并避免攻击者滥用该系统，提交争议和上诉需要仲裁费用。 每个陪审员将获得解决争议子厅所确定的费用， 仲裁智能合约将决

定哪一方支付仲裁费用。简单的方式比如争议的提交者或上诉方支付费用， 但是我们可以采用更加完善的激励机制。 例如：

- 在争议裁决中，各方将在智能合同中存入相当于仲裁费用的金额。 如果一方不这样做，智能合同将裁定支付仲裁费的一方（甚至不产生上诉）。 如果双方存入资金，当争端结束时，获胜方存入的仲裁费用将得到退还。
- 在上诉中，双方都必须交存仲裁费。 上诉人还必须按照上诉费用的比例存入额外的费用，这些费用将发给胜诉方。 通过这种方式，如果一方进行轻微的上诉损害对方的利益，对方将获得时间损失赔偿，而如果上诉成功，该费用将被返还给上诉人。

更多的仲裁智能合约如何定义分配仲裁费用将会在以后的开发中继续完善。

4.5. 上诉

如果在陪审团做出决定后，一方不满意（因为它认为结果不公平），它可以上诉并再次提出新的争议。每个新的上诉实例将有两倍于以前的陪审员数量上再加一个。由于陪审员人数增加，上诉费将为：

上诉费=新的陪审员数量*每位陪审费 - 已支付的费用

如果判决被上诉，该争议的陪审员先不能获得支付（但由于令牌重新分配，他们仍然受到争议的影响）。这会激励陪审员对他们的裁决进行解释。如果给出了适当的解释，各方就不太可能提出上诉，因为更充分的解释让他们相信裁决是公平的。由于向每名陪审员支付仲裁费用，并且陪审员人数增加，因此仲裁费用随着上诉数量呈指数增长。这意味着，在大多数情况下，各方不会上诉，或只会上诉一定的次数。然而，不限制上诉次数可以预防攻击者贿赂陪审员（参见反贿赂部分）。

4.6. 激励系统

陪审团裁决争议可以获取仲裁费。并且在争议结束后，表决与多数不一致的陪审员将失去一些令牌，被分配给其他表决多数的陪审员。这样可以对他们进行诚实裁决给予激励。

在Kleros就争议作出裁决之后，令牌将被解冻并在陪审员之间重新分配。再分配机制受到SchellingCoin（参见2 早期理论：谢林币原理）的启发，其中陪审员根据其投票是否与多数陪审员一致而获得或失去令牌。

如果投票赞成多数选择的选项，我们将假定评审团成员投票连贯一致。投票不一致的陪审员失去的令牌数量为：α·最少激活·权重。α参数决定了裁决后要重新分配的令牌数量。这是一个内生变量，来源于投票环境的内部变数产生的监管机制。

最少激活参数是可在子厅中可激活的令牌的最小数量。

激励令牌在多数票陪审员之间按其权重成比例地分配。更加完善的分配方式将会在以后的研究中发布。图4显示了一个令牌重新分配的示例。陪审员可能无法提供他们的投票，为了预防这种行为，无法提供投票的惩罚是不一致投票惩罚的两倍（α·最少激活·权重）。这激励陪审员尽量提供他们的投票。

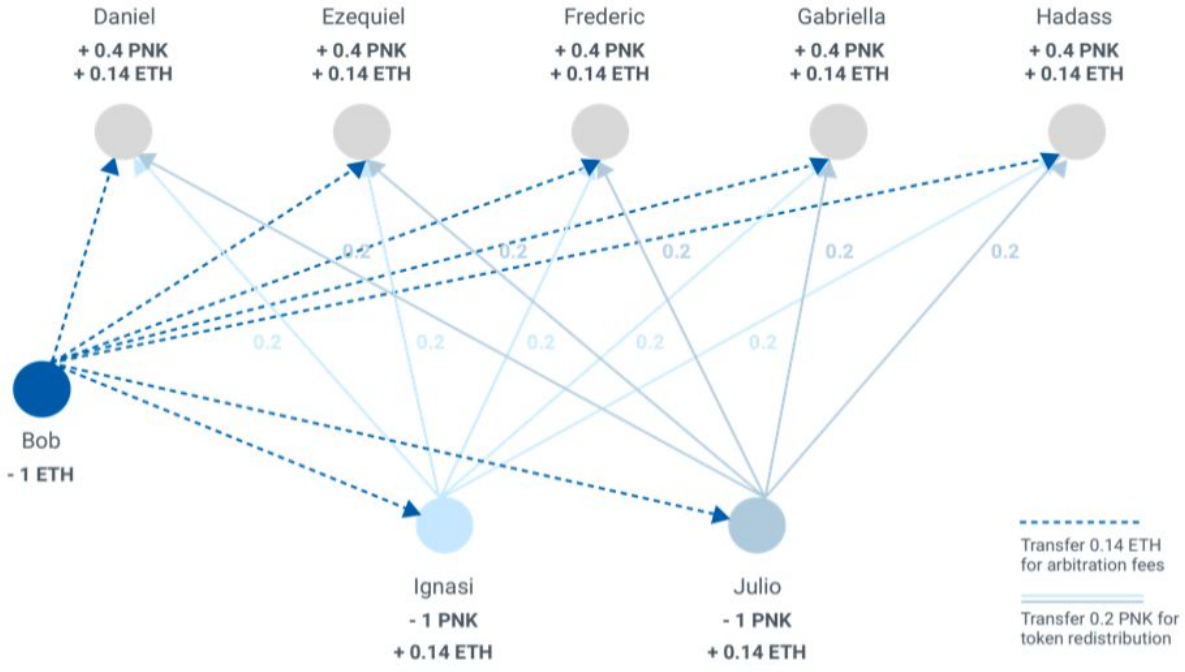


图4：七名陪审员进行投票后，令牌重新分配。令牌被重新分配给多数票陪审员。鲍勃失去了争议并支付了仲裁费用。其他预存款退还给有关方。

在上诉的情况下，根据最终上诉的结果，令牌在每个级别重新分配。如果在某个级别上没有多数票，这些令牌就会被分配给胜诉方。

当不存在恶意攻击时，各方都会被激励投票给真实的想法，因为其他方会选择真实的，进而实现投票的诚实和公平。Kleros认为谢林点是诚实和公平的。有人可能会认为这些决定是主观的（例如，用来预测市场的谢林币机制），则不会出现谢林点。在（参考文献18）中，托马斯谢林所进行的非正式实验表明，在大多数情况下，由多方投票的Schelling Point不存在。但他发现有些选择比其他选择更有可能被选中。因此，即使一个特别明显的选择不存在，一些选择将被认为更有可能被其他方选择并且将被有效地选择。

我们不能期望陪审员100%的时间是正确的，因为到目前为止，尚未有任何仲裁程序可以实现这点。有时，作出正确裁决的陪审员可能会失去令牌。但就整体而言，只要他们的损失低于获得的仲裁费用，系统将正常运作。

4.7. 预防恶意攻击

4.7.1. 多数攻击

如果一方（或多方一起）要购买一半的令牌，它将控制总厅的结果，因此最终可能会决定所有结果。 然而，如果他们购买了一半以上的代币，那么这些代币的公平分配是不太可能的。

首先，要有一半的令牌出售 - 这是不能保证的。 此外，一方可以以当前市场价格购买这么多代币并不意味着它可以购买其中的一半。 与大多数实物资产相反，令牌的边际成本不断上涨。 它们将在交易所动态定价，如果一方购买量加大，价格将因市场深度而上涨，从而使其获取代币的成本越来越高。

4.7.2. 贿赂攻击

上诉是反贿赂的重要机制。贿赂一个小陪审团是相对容易的。但由于受害者始终有上诉的权利，攻击者将不得不以不断上涨的成本贿赂越来越大的陪审团。攻击者必须准备花大量的钱贿赂陪审员，一直到总厅，最后很可能会失败。

为了控制整个判决，攻击者需要贿赂持有总数超过50%的PNK。这种攻击在绝大多数模型中不起作用（其中超过一半的令牌由不接受贿赂的诚实方控制）。但即使是不诚实的多数人（比如大多数令牌持有者只追求利润最大化），该系统也可以在一定条件下抵御贿赂攻击。
总厅的成功贿赂会大大降低令牌的价值（谁会希望他的合同由不诚实的仲裁机构进行仲裁？）。

因此，攻击者要能够提供超过价格下降预期损失50%的价值，以便他的贿赂获得成功（几乎在所有情况下，这个数字都将超过争议中的获利值）。实际上，上诉至总厅的可能性及其低。然而，只要存在可能，就需要激励机制。

更精细的攻击（P + epsilon攻击）也是存在的，承诺只有在攻击不成功时才支付贿赂。这种攻击需要很高的预算，但如果成功则成本为零。然而对于这种攻击，有一种博弈理论反应，即陪审员使用混合策略（陪审员只接受贿赂的概率与接受贿赂相比增加了他们期望的奖励）。
（参考文献9）中可以找到关于这种攻击和响应的更多细节。

4.8. 裁决厅结构

在注册成为陪审员时，用户可以从普通庭开始，根据他们的技能选择特定庭。 每个子厅均具有特定的政策，时间，费用，抽取的陪审团成员数量和激活的令牌。 每个令牌持有人最多可以注册在一个子厅内。 图5显示了注册的例子。

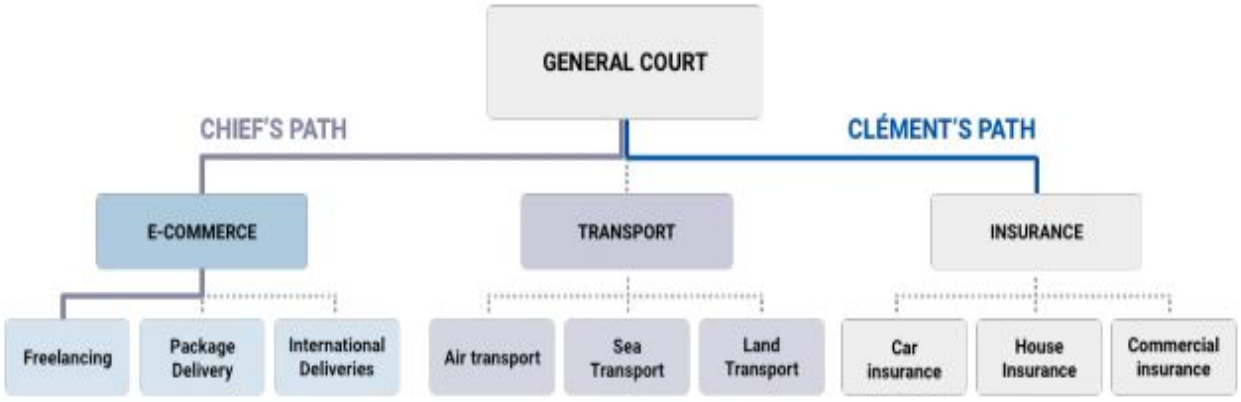


图5：陪审员选择子场示例。 Clement可以在总厅和保险子庭中担任陪审员。 Chief可以在总厅，电商庭和自由职业厅担任陪审员。

要求陪审团在分庭之间做出选择，可以促使他们选择他们最擅长的分庭。如果他们能够自由选择每个子厅，一些人会利用他们拥有的大量令牌选择所有子厅从而获利，我们希望令牌是裁决的工具而不是以获利为主。

4.9. 监管机制

随着Kleros协议的推广和用户的增加，会需要创建新的子厅，会调整子厅政策和控制参数，也可能为平台添加附加功能。 令牌持有人使用流动投票机制来决定子厅的变动（参考文献13）。 令牌持有者的票数等于他们持有的PNK数量。 他们可以选择直接投票或授权投票。 当用户未投票时，他的投票权自动转移给他的授权代表。

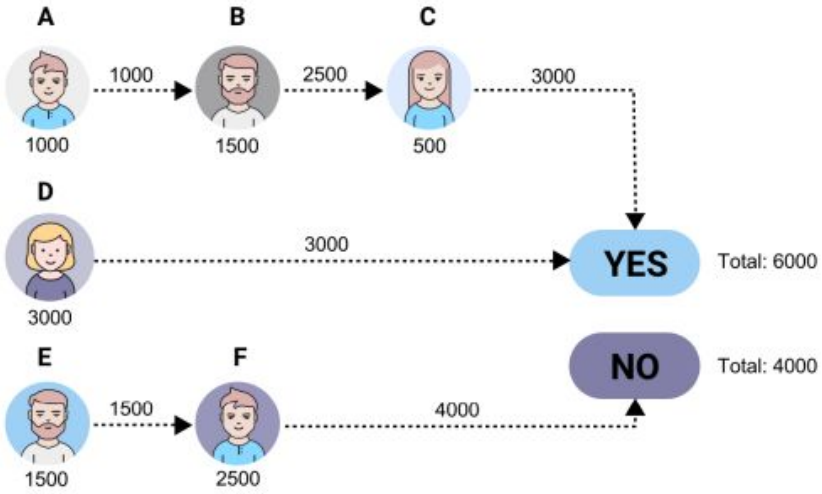


图6.投票委托可能是子厅内有效。 用户可以选择只在一些子厅内委托他们的投票。 被委托方可以是执行任意复杂投票规则的智能合约

（例如根据市场数据对更新费用进行投票）。

治理机制可用于：

1.制定政策：

政策是关于如何仲裁争议的指导方针。 它们相当于传统司法系统中的法律。 他们决定哪一方应该在特定条件得到满足时获胜。 它们可以是特定的子厅专有的。

2.修改子厅：

（a）增加子厅

（b）删除子厅

（c）修改子厅等级

3.修改子厅控制参数：

（a）仲裁费用

（b）每场裁决的时间

（c）最少的激活令牌

4.更改Kleros所依赖的智能合约：

Kleros协议如果需要改进，令牌持有者可以通过投票对协议的智能合约进行改进或采取紧急措施。

5. 应用程序

Kleros是一种通用的多用途系统，可用于多种如下可能的应用示例：

•第三方托管：

为了支付脱链商品或服务，可以将支付款置于智能合约中。

收到货物或服务后，买方可以将资金解锁给卖方。如果有争议，Kleros可以通过智能合约决定退款回买方或者支付给卖方。

托管可以扩展到很复杂，比如一个租赁协议，承租人可能需要支付押金。如果财产损坏且承租人不同意赔偿，业主可以提出争议，从保证金获取赔偿。

•微型任务：

去中心化的平台适合小额支付任务（以Amazon Mechanical Turk（参考文献 1）的方式）。工作人员会提供保证金并提交微型任务的答案。提供正确答案的工作人员将从提供错误答案的工作人员保证金中获取部分激励，

•保险：

保险人将向保险公司支付费用，以便在发生特定事件时获得赔偿。保险公司必须对所有参保人员提供保证金（尊重风险管理规则）。发生保险事故时，保险公司可以对其进行验证并赔偿保险人。如果保险公司认为该事件不符合保险条款，则会与参保人发生争议。如果保险公司胜诉，则保险公司保证金中的资金将返还给保险公司。如果保证金与多个参保人相关联，而且多个参保人的索赔超过保证金，则还需要新的争议解决程序来确定如何将这些资金分配给参保人。

•Oracle：

智能合约使用的分散数据流是以太坊早期设想的用例之一（参考文献 7）。一方（可以是一个智能合约）提出一个问题。每个人都可以使用令牌参与并提交答案。如果每个人都给出相同的答案，Oracle将返还所有令牌。如果有多个答案，将进入争议解决程序。Oracle根据争议解决过程中给出的答案，将错误答案的参与者令牌分配给提供正确答案的参与者。

•策划名单：

策展名单可以是白名单或黑名单。例如，白名单可以列出已经过适当审计程序的智能合同。黑名单可以列出在ENS（以太坊名称服务（参考文献 2））注册但是与其名称无关的名称（例如，恶意方可以注册“kleros-token-sale.eth”，以骗取人们发送资金到那个地址）。令牌持有者可以通过投入保证金提交加入名单的名称。如果在规定的时间内没有人提出异议，则该名称将加入名单，保证金令牌退还给提交者。如果有反对者在此段时间内通过使用令牌保证金提出异议，则启动纠纷解决程序。如果提交者胜诉，则该名称被添加如名单并且提交者获得反对者的令牌押金。否则，反对者将收取提交者的令牌押金。

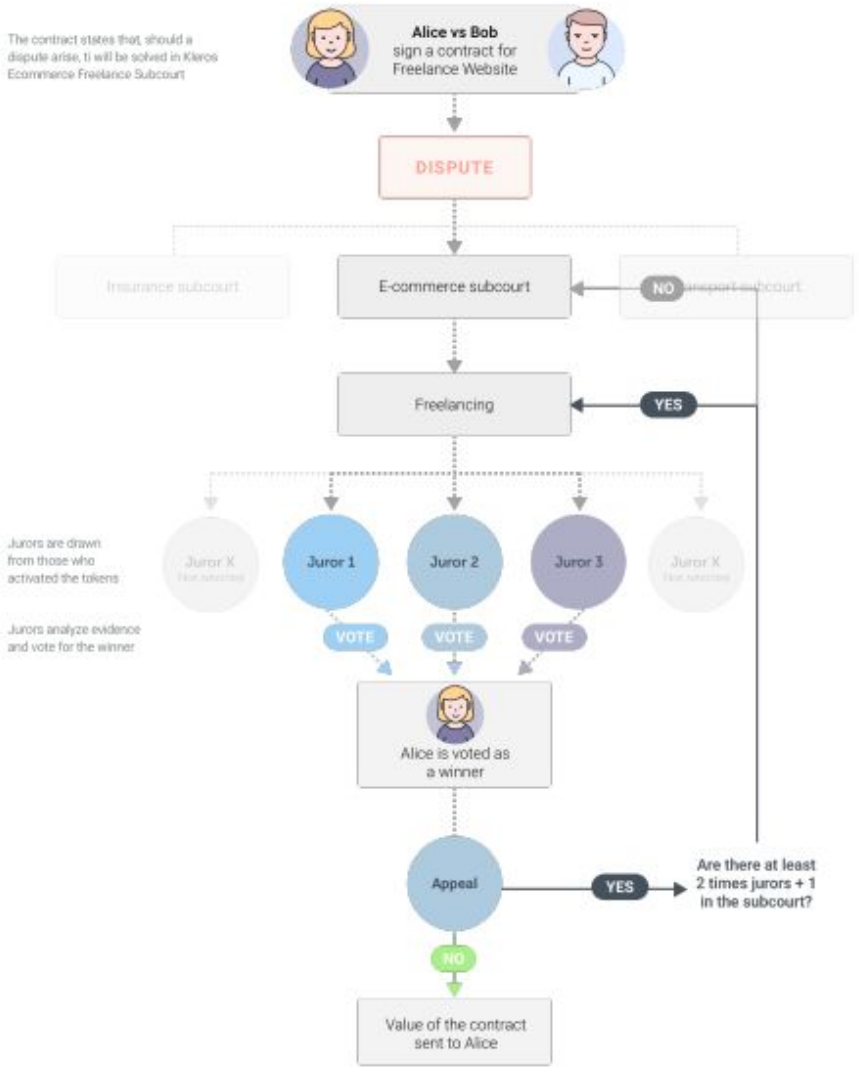
•社交网络：

防止垃圾邮件，诈骗和其他滥用是去中心化社交网络的一大挑战。各方可以举报违反网络政策的行为并提交令牌押金。如果被举报者提出争议，则启动争议解决程序。如果被举报者胜诉，举报者令牌押金将被分配给被举报者的。如果举报者胜诉，智能合约可以采取诸如：删除内容，被举报者损失注册令牌押金，被举报者社区行为被限制等等措施。

6. 结论

Kleros是一个去中心化的裁决系统，

通过众包陪审员，依靠激励机制来执行仲裁智能合约。



数字经济的兴起使得劳动力，资本和产品市场更加国际化和实时化。 P2P经济需要快速，经济，去中心化和可靠的纠纷解决机制。 Kleros使用博弈论和区块链实现多种用途的仲裁协议，能够支持大量的电子商务，金融，保险，旅游，国际贸易

，消费者保护，知识产权和学术界等众多应用。加密货币提供了一个以安全的方式支付和收款的可能。加密货币正在使得数百万人融入到现代化的金融领域。

Kleros正在裁决方面也会实现这个目标，就是通过在大量合同中进行仲裁，从而无需支付高额的实体法庭费用。就像比特币带来了“为无法获得传统金融机构服务的人提供金融服务”一样，Kleros有可能为“为无法获得公正的人提供公正”。

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] Blum, M. Coin flipping by telephone a protocol for solving impossible problems. SIGACT News 15, 1 (Jan. 1983), 23–27.
- [5] Boneh, D., Lynn, B., and Shacham, H. Short signatures from the weil pairing. Journal of Cryptology 17, 4 (Sep 2004), 297–319.
- [6] Brassard, G., Chaum, D., and Crepeau, C. ´ Minimum disclosure proofs of knowledge. J. Comput. Syst. Sci. 37, 2 (Oct. 1988), 156–189.
- [7] Buterin, V. Ethereum, a next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper, 2014.
- [8] Buterin, V. Schellingcoin: A minimal-trust universal data feed. https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/, 2014.
- [9] Buterin, V. The p + epsilon attack. https://blog.ethereum.org/2015/01/28/ p-epsilon-attack/, 2015.
- [10] Buterin, V. Introduction to cryptoeconomics. https://edcon.io/ppt/one/Vitalik%20Buterin_Introduction%20to%20Cryptoeconomics_EDCON.pdf, 2017.
- [11] Bunzy, B., Goldfeder, S., and Bonneauy, J. ¨ Proofs-of-delay and randomness beacons in ethereum.
- [12] Douceur, J. R. The sybil attack. In Revised Papers from the First International Workshop on Peer-to-Peer Systems (London, UK, UK, 2002), IPTPS ’01, Springer-Verlag, pp. 251–260.
- [13] Ford, B. Delegative democracy. http://www.brynosaurus.com/deleg/deleg.pdf, 2002.
- [14] Friedman, D. A positive account of property rights. Social Philosophy Policy 11 (1994).
- [15] Laudan, L. Truth, Error, and Criminal Law: An Essay in Legal Epistemology. Cambridge Studies in Philosophy and Law. Cambridge University Press, 2006.
- [16] Peterson, J., and Krug, J. Augur: a decentralized, open-source platform for prediction markets. http://bravenewcoin.com/assets/Whitepapers/Augur-A-Decentralized-Open-Source-Platform-for-Prediction-Markets.pdf/, 2015.
- [17] Reitwiessner, C. From smart contracts to courts with not so smart judges. https://blog.ethereum.org/2016/02/17/smart-contracts-courts-not-smart-judges/, 2016.
- [18] Schelling, T. C. The strategy of conflict. Oxford University Press, 1960.
- [19] Sztorc, P. Truthcoin, peer-to-peer oracle system and prediction marketplace. http://www.truthcoin.info/papers/truthcoin-whitepaper.pdf/, 2015.