

# BitShares PLAY 非技术白皮书

## 1.0 介绍

BitShares PLAY(简称 PLAY) 运用区块链技术，试图建立一个去中心化的和自治的游戏平台。第三方可以基于此平台开发多种可证公平的游戏，包括一些从未有过的独特类型。这些游戏兼具娱乐性和公平性。同时 PLAY 的随机数生成器功能（技术实现详见附录）和自定义资产及交易功能可被第三方游戏开发商接入，为第三方游戏的公平性和资产发行及交易提供便利和技术保证。

## 2.0 PLAY 功能

### 2.1 PLAY 平台支持的链上游戏类型

链上游戏是指游戏的全部逻辑都在区块链上定义并运行，不依赖于区块链之外的其他中心化机构（无外部的信任隐患）的游戏。

#### 2.1.1 基于概率的游戏

典型的如 Dice, Chance Coin 类游戏。

#### 2.1.2 趣味竞猜类游戏

关于某一件事未来是否会发生或如何发生的竞猜。例如，名人是否会在一个时间点之前结婚或离婚。外部事实发生后，信息需要输入区块链。在基于 DPOS 的 BitShares PLAY 中，可由受托人投票来完成这个任务。由于受托人是由 PLAY 持股者投票选出的，我们认为受托人投票的最终结果会是可信的（如果投票结果与事实不符，其后果由选举这些受托人的人，也就是全体 PLAY 持股者共同承担，在此意义上仍然是公平的）。

#### 2.1.3 投票驱动型的多人竞技类游戏

这是由 ByteMaster 提出的一种全新类型的互动游戏。举例来说，例如国际象棋。区别于传统的二人竞技模式，在 PLAY 上，用户分成两组。例如每个 ID 具有一个颜色字段，当前是黑组与白组用户竞技。轮到一方出招时，该组用户均有权按自己的想法出招，其权重等于该用户 ID 下的余额，最终这一方按照累计权重最高的着法执行，也即由该组用户投票决定。

这是一种前所未有的独特类型的游戏，即使在数字加密货币领域内也是首创。

#### 2.1.4 棋牌类游戏

该类游戏包括简单的棋类对弈游戏，也可能会探索一些桌游和扑克类游戏的可能性。

#### 2.1.5 概率与策略相结合的竞技类游戏

该类游戏是 2.1.1 类和 2.1.4 类游戏的综合体，具有运气成分同时也具有策略成分。类似的有 Cannot Stop 和 Bingo。

## 2.2 去中心化的游戏资产定义和 P2P 交易市场

传统的游戏中一般都会有游戏币和游戏装备的概念。PLAY 具备用户发行自定义资产的功能。这样游戏开发商可以在 PLAY 平台上发布自己的自定义资产（可以是游戏币，也可以是装备类物品），然后在自己的游戏内部支持这些资产的充值和提现，或者直接读取 blockchain 上的资产账本以实现控制总量上限。同时 PLAY 提供这些资产的交易功能。玩家可以在 PLAY 的市场上自由买卖这些资产。通过这种方式，建立跨越不同伺服和游戏的 p2p 经济系统，取代传统游戏的自发行方式。

如果在 2.1 所述的链上游戏获得了极大的用户基数，可以预想游戏开发商会很想在 PLAY 平台上发行自己的资产来吸引用户的注意。届时可以引入发行自定义资产的资格竞拍等功能。当然这只是盈利模式之一，事实上当用户基数很大时，还可以有很多其他盈利模式。

PLAY 鼓励将市场以内置的方式接入传统游戏之中，这样用户就无需认识第三方平台，就可实现游戏资产的去中心化交易。

## 3.0 PLAY 内置的随机数生成器算法简介

随机数有很多的应用场景，而随机数的生成是一个由来已久的问题。一个广泛的原则是：随机性的生成最好不被任何个体所控制。因此譬如从比特币的未来某区块的数据来获取随机性的方式是不能使人信服 的，因为这些随机性最终实际上是由某个个体决定的，无法证明这个相关人没有作恶。

PLAY 采用的是一种分布式的随机数生成算法，使用了 DPOS 结构中的受托人來提供随机性。受托人事先生成私密的种子数据，然后生成区块时公布该种子数据的哈希值，在下次生成区块时再公布该种子数据。最终外部过程所使用的随机数由连续的多个（至少应大于等于 101）种子数据来确定。这样只要有一位受托人是诚实的并将他们的信息保密，那么其他人就无法预测结果。那么我们可以很放心地假设 受托人中至少其中有一个是诚实的。这样产生的随机数可信程度是非常高的。

## 附录：

开发路线图

- A 基本的资产转账和 ID 功能, CP 账户，内置兑换模型和交易模型
- B 链上游戏平台支持(包括 1-2 个链上示例游戏)，自定义资产以及充值提取，读取 API 等功能
- C 轻钱包功能
- D 趣味竞猜类游戏的游戏平台支持，第三方游戏开发者接入