去中心化点对点游戏资产平台,
可运用智能合约整合中心化游戏和预测市场

hackfisher@gmail.com

2014-08-04

翻译：浮壹白Allen，麥克貓，HeyD, HackFisher

1.0 介绍

比特股Play（后面统称PLAY）作为一个实验产品，它将展示和验证如何实现建立一个去中心化和自治的游戏资产平台。此平台拥有多种可证公平的猜测或概率类游戏为产品特征，以及拥有整合各种第三方游戏和资产系统的能力。PLAY的数字股份（PLS），并结合了内置的、第三方游戏的资产，建立出一个自由的市场和兑换平台。这类系统也被称之为去中心化自治公司（DAC）。

游戏资产平台的基本理念是它包含了一个默认的内部兑换模式。在PLAY中的每种游戏资产都是一个合约的组成部分，这份合约包括系统定义的资产供应量以及发布股份所需的PLS抵押率。通过抵押PLS可以发行游戏资产，也可以通过收回PLS来销毁游戏资产。资产股份的价格取决于用当前总供应量和当前抵押品来定义资产的合约。所以，游戏资产的总供应量机制同样也是系统内合约的一部分。对于内置的游戏来说，总供应量的变化规则是DAC共识的一部分。

概率类游戏几乎全部依赖于可信的第三方来提供随机源。尽管基于中心化信任模式的系统运作良好，但是玩家作弊的可能性对于系统来说是一种威胁。虽然一些基于加密货币的在线游戏支持经过公开验证的随机源，但是玩家还是可以通过选择性提交交易来作弊，因为他们事先知道随机源的秘密。从这个角度来看，玩家只能被迫相信游戏开发者是正直的，这降低了这些游戏的销路，并阻止了那些不相信开发者的人们来玩游戏。

PLAY游戏币（CHIP）并不只是内置的游戏才能使用。它还能被第三方游戏当成经济系统模块来集成，甚至包括中心化的游戏，只要提供能够满足PLAY的内部游戏资产交易所的需求的合约就可以。合约可以是DACs内部或之间的共识，也可以是一个DAC和中心化游戏之间的智能合约。这可以通过采用像智能神谕或Orisi那样的智能合约技术来实现。

2.0 系统代币

PLAY股份（PLS）是系统内的代币。PLS主要是用来作为PLAY系统的虚拟股份，同时也是作为分红的依据单位支付利息给PLS持有者，以及可以用来支付给运行系统的托管人(Delegate)。其次，PLS是作为用户购买游戏币去玩游戏所使用的代币。PLS提供了一种改进代币分配方式的新形式，并可能探索出一种用代币奖励游戏赢家的新模式。

在系统中还有其他类型的代币，比如各种游戏币，包括了用户发布的资产和有PLS背书的游戏币资产等。PLS背书的资产（游戏币）在系统内比较特殊，游戏币被创建或销毁，是系统根据市场当前价格的增加或收回PLS保证金决定的，表现为玩家用PLS兑换成游戏币或者用游戏币兑换成PLS。详细一些来说，价格是由当前PLS保证金占总游戏币供应量的比率决定的。这意味着游戏币的供应量会根据用户对于游戏中的需求而有所变化。随着游戏变得能够获利和越来越流行时，那么就有让越多的PLS为游戏中增加的游戏币做抵押金背书。与此同时，游戏币不会凭空生成，因为每一个单位的游戏币都是有PLS背书的。当游戏币销毁时，这些PLS将会被返回给系统。初始抵押金和供应量是游戏开发者设定的，同样价格亦是。当价格被设定，游戏创建者就再也不能修改。游戏币的价格是根据当前所有的PLS抵押金总量和游戏币的总量计算出来的，同时基于区块链的透明的游戏规则可以对游戏所拥有的抵押金和游戏币进行分配。系统中就会有不同种类的游戏币，正常来说，每一种游戏币会对应一个游戏，否则，系统则需要达成新的游戏币间的共识。

人们可以用PLS并在系统内部兑换为游戏币，然后用于玩游戏。所有花费掉的游戏币会当成奖励返回给玩家，当是也可以选择一小部分作为系统优势而得的利润作为奖励返回给游戏创建者或者系统受托人。系统的所得被受托人们管理，他们可以留作运营费用或捐献出来。其中一部分也可以销毁掉，这样相当于给PLS持有者们分

红。在这个系统中，功能和正直的受托人们一并运行，不会有任意一个中心化实体能够从系统所得中获得好处。

PLS的作用不仅限于兑换游戏币，其本身也可以作为投资资产目的。玩家也可以在开放市场中交易PLS来玩游戏，但不以投资为目的。这两种行为都会导致对PLS的需求，并因为持有PLS而获益。

PLAY的游戏币(CHIPS)资产提供了一种良好的经济模型，能够保护用户的游戏资产免于被稀释。因为平台必须找到一种方式来保证新发行的游戏币必须有相应的PLS股份作为抵押金背书，或者在PLAY中以硬编码形式写入游戏合约的规则和机制。PLAY中的游戏不应该被赋予基于信任的随意发行游戏币的能力。

2.1 PLS和游戏币之间的内部交易模型介绍

游戏币不同于比特股X市场中发行的类BitUSD资产和用户发行资产。PLS和游戏币之间有一个固定价格兑换模型，没有市场挂单和撮合交易的概念，是比特股PLAY系统共识中的一部分。

每种游戏币资产都需要一部分PLS作为抵押金而创建生成的，总量会被记录在系统中。在创建之后，这部分PLS会被作为冻结的抵押金存在于系统的余额中。

游戏开发者可以根据它们的需要将经济模型写入游戏系统中，但是总供应量和PLS抵押金的相关规则必须要透明化。根据PLS抵押金和游戏币供应量之间的比例，确定游戏币和PLS之间的系统兑换价格公式。

1 游戏币 =（PLS抵押金总量/游戏币总供应量）* 1PLS

这意味着任何人都可以在当前区块的价格下从系统那里兑换买卖（换句话说即是创建/销毁）游戏币，用来买游戏币的PLS将会被增加到对应这些游戏币的抵押金中，兑换而来的游戏币将会增加进游戏币总供应量。在每个新增区块中，根据PLS抵押金供应量和游戏币供应量的更新，价格都会被重新计算。

在这种模型下，越受欢迎的游戏将会有越多的抵押金，而那些销毁更多的游戏币的价格会上升，以此产生利润（相对于PLS或其他资产而言）。游戏币资产也可能被稀释，但不同于无控制或无节制的稀释，如腾讯的Q币。游戏和PLAY之间的合约、总供应量和稀释规则都必须以硬编码形式写入合约规则中，以此保证绝对透明。

为了让游戏币成满足上面交易模型的约束，每个游戏的合约中需包含：

1、 可证明的游戏代币总供应量。
2、 和第三方中心化游戏整合，PLAY中的游戏币和游戏原生系统之间1：1转化的方式，或运用跨链交易或支持系统托管方式。最简单的方案是在PLAY系统内置游戏，或采用PLAY区块链作为该游戏的资金记录单。

3.0 采用DPOS（授权股份证明机制）作为共识算法

加密货币技术和区块链概念来自于中本聪的“比特币：一个点对点的电子现金系统”，创造了一个分布式和无需信任的总账，允许账户存在。像工作量证明（POW）那样的公式算法和DPOS机制都需要更新并维持网络和公共总账，并同时保持系统安全和稳定。

DPOS的优势在于更快的区块确认和可扩展到VISA级别的每秒10000次支付或转账频率。同时，系统依然是去中心化的，既不会被某个个体破坏也不会被某个个体控制。受托人们的工作很简单，就是签署区块，如果他们没有履行义务，那么可以被随时开除。这样，股份持有者们可以共同达成全面共识。而鉴于在传统POW体系下，只有挖矿者才能制定网络中的共识，所以不挖矿的股份持有者并不能参与共识的制定。

受托人运行这个去中心化的系统，让一切发生。他们存在于去中心化系统中的关键意义在于人们可以投票来决定谁来提出目前系统中的共识，或修改它。这可以帮助系统升级和自我改良。
在DPOS点对点（P2P）游戏系统中，受托人的角色更加重要，因为他们不仅是收集交易信息、按照计划时间点签署出块，还提供公平证明和在游戏中使用随机分配秘钥，基于申请投票的接收新的游戏进入系统。在4.2段落中有更多细节。

4.0 去中心化系统中的真正随机数产生算法（RNG）

4.1 RNG概览

- **由可信的第三方提供**

在游戏领域，一种最常见的做法是直接使用现有的彩票出奖结果作为随机数据源，如采用纽约大乐透快速开奖彩的中奖号码。但其实这并不可靠，因为提供源可以被修改，人们甚至无法证明它不是预先就被选中的，这就意味着拥有内部渠道的人可能会修改这个结果。如果玩家必须相信某个可能作弊或者失效的个体，这无疑是非常危险的。

- **中心信任实体使用的可证明秘钥**

理想的情况下，随机数生成器的随机性应该是可被证明且事前无法被预测的，同时它又是确定且事后能很容易被重现以验证的。P2P网络的节点或玩家应该能够在开奖之后验证随机数生成器是否公平。

一种可供验证的方式是通过事先公布随机选定的密钥的单向哈希值，在下一个区块产出，密钥被公布之后，参与者可以验证这个哈希值。

通过委派给一个中心信任实体，这项工作便可以很容易地实现，但此方法有一个缺陷：任何一个知道了密钥的实体（如经典的中本聪骰子）都有可以通过提交经过挑选的交易来舞弊。因此，中心实体相对于其他玩家而言有相对优势，密钥对于他们来说并不是那么地随机，他们可以利用这一点。需要相信一个实体能长期持续地保持诚实，无疑是一个严重的缺点。

- **未来事件**

另一种方式是以未来的某些事件作为随机数的结果。对未来事件随机性的定义和公布可以同时发生。但是这些事件应被仔细地甄选，因为存在可能某些个体可以对未来事件的结果产生影响。可以通过选择那些难以被影响和预测的未来事件来解决，或者通过减弱个体对这些未来事件的影响力（如增加影响因子的数量）来解决这个问题。

有一些未来事件，如放射源，是很难甚至是不可能去预测或计算的。它们的定义和发生可以是在同一时间点，然后立刻被公布（无需计算），而不会被干涉。

- **利用区块链的随机性**

我们可以引入工作量证明（POW）来增加玩家干预随机数生成器的难度。这样可以使玩家的因子更独立，防止串通或者让舞弊在经济上不可行。一般来说，若某个玩家拥有巨量的算力，那么相比于通过彩票中奖来获利可能性，通过挖矿获取收益的概率会更高。

例如，可以通过经由将某些游戏数据散列为加盐值，并结合比特币区块数据的哈希值生成一个聚合的值，以这个聚合值来产生随机数。 比特币挖矿具有的随机性会增强这个随机数生成器的安全性。

假如某个矿工得出某个区块后不对外广播，而是重新选择，那他会失去相对其他矿工的竞争优势。矿工看到结果之前的那段时间，不能构成他挖矿的优势。这也是经济上不可行的原因，工作量证明降低了矿工对时间成本的影响力。更深入地看，试图去碰撞也是很困难的，因为概率空间大于47612（赢取双色球的三等奖），假如某个矿工在其他矿工将区块广播出去前有多达10倍的时间，概率依然小于1/47612。

所以，基于挖矿的方式提供了一种去中心化的随机因子，可能足以启动一个DAC。但事实上，即便在POW的帮助下，矿工依然有攻击的可能。矿工或者矿池管理员有可能通过有选择性地忽略对他们不利的区块进行舞弊。随机性的生成最好不被任何个体所控制。

- **可证明的分布式随机数产生算法**

POW可创造一种竞争性的环境，每个参与者（矿工）无法干预随机数结果，或者至少无法在经济上有利可图。若不使用POW，我们可以使用一种将随机数产生的因子分布到尽可能多的个体，从而让每个个体都无法舞弊的方法。简单来说，想象一下这些个体都是理事会成员，他们事先生成私密的随机数，然后向全网公布哈希值。在生成了指定的抽奖区块后，所有的理事会成员都公布密钥。这些密钥再与抽奖区块的头部数据一起进行哈希计算。

这种特定结构的理事会将远在全网知道抽奖区块的哈希值之前，就提交了他们的密钥。操纵抽奖的唯一途径就是所有理事会成员串通。只要有1位成员是诚实的并将他们的信息保密，那么其他成员就无法预测结果。成员的数量越多，就越难串通。

4.2 从DPOS产生的可证明分布式随机数生成算法

可证明分布式地提供密钥的方法可以产生一个真正的随机数生成器 (RNG)算法. DPOS就是使用了这样的RNG算法, 其中受托人的顺序每个回合都会随机洗牌.

整个流程可以拆解为以下步骤, 其中不需要“董事会”。

1. 想要为随机数产生做出贡献的人提供密钥的哈希值 HASH(*S*).
2. 在所有的HASH(*S*)已经公布之后, 所有的参与者都要提供S
3. 所有的参与者提供S之后, HASH(*S[0...N]*) 会被算出来当成选定的随机数

任何担忧结果的随机性的人可以发布两次转帐就可以参与这个过程. 每个人都可以轻易地选择相信其他没有勾结的人们. 只要整群人当中只有一个人是诚实的, 那么结果就会是随机的. 如果全体董事会成员都参与其中, 那么我们可以很放心地假设至少其中有一个是诚实的.

让101位受托人担任RNG董事会成员十分地平衡, 而这也将提供可证明的安全的成本分摊到最在乎这件事情的人身上. 这表示我们会让董事会成员负责抽签, 因为他们有99%上线时间保证来进行RNG, 并且大致上值得信赖. 只要其中的一位是诚实的, 那么结果就会是真正的随机.

“分布式”意味着一个区块的随机数事由前一轮101位受托人所提供的密钥产生，只要至少其中一位是诚实的，结果就会是真正的随机. “可证明”表示他们需要在下一个回合发布密钥的哈希值到区块链. 根据密钥所得出的哈希值必须和之前发布的哈希值相同. 由于两者必须一致, 因此受托人不可能通过公开不诚实的密钥来作弊.

因此在DPOS中, 我们可以透过以下的伪代码 (包含了固定数量的受托人)来阐述:

Code:
代码：

```
struct Block
{
  hash  HASH( S[n] ) // where n is the index of secrets generated by this delegate
  hash  S[n-1]
```

```
};
```

每个区块中的头部中包含一个HASH(*S[n]*)，其中*S[n]*是这个受托人下一次生产区块时将揭晓的密钥．同时当前区块也包含上一个区块的秘钥*S[n-1]*.

We now have a stream of secrets being revealed once per block (15 to 30 seconds)... from this stream of secrets we can generate the random number R for the block as:
如此一来, 我们就有了密钥的串流, 每隔一个产块间隔 (15-30秒)就会提供一组密钥。从这个串流我们可以用以下方式产生区块的随机数R:

Code:
代码：

```
if( first_block_produced_by_delegate ) then Block[HEAD].revealed_secret = 0
ASSERT( HASH( Block[HEAD].revealed_secret) ==
 GetLastBlockProducedByDelegate(Block[HEAD].delegate_id).secret )

R = HASH( Block[HEAD].revealed_secret )
for( uint32_t i = 1; i < 100; ++i )
{
    R = HASH( Block[HEAD-i].revealed_secret + R) // where + is concat
}
```

当中区块所产生的随机数以R表示

每个R都是经由100位受托人所提供的密钥所得出. 如果当中至少有一位受托人是诚实的, 那么产生的R就会是真正随机的.

实际上, "`Block[HEAD].revealed_secret`"就是上一轮HEAD的受托人所产生的*S[n-1]* (每个回合会有一百个受托人所产生的区块). 如果我们需要至少"如果当中至少有一位受托人是诚实的, 那么产生的R就会是真正的随机"这样的安全性， 大奖就应该使用第100个区块的R来抽出, 此时距离购买彩票的交易已经间隔了100个区块.

这样一来每个人都可以简单地确认公平性, 并接受其他人都可能是串通的风险．在牵涉到机率的游戏里, 你可以让每个参与的游戏交易都有自己的密钥，一旦买票窗口关闭, 每个人可以显示他的密钥。所有密钥的哈希值就可以成为游戏结果(比如中奖号码)，由于没有任何有效的交易会被董事会排除在区块链之外一到两个回合，我们可以安全地假设没有人知道最后会产生出来的随机数是什么。 但是这样一来随机算法的过程就会牵涉太多的游戏过程, 因此收集所有的密钥的时间可能会很长, 可能无法保证所有的密钥会在游戏结束之前收集完成。

4.3 DPOS中的轮值洗牌

当101位受托人都签署了区块之后DPOS就会洗牌，受托人的顺序便根据随机数随机洗牌．这种方式可以让去中心化的共识过程避免恶意受托人攻击．每个受托人在轮到他的时候就只能选择是否要发布区块 (也就是给出密钥)．如果没有洗牌的过程，恶意的受托人就可以藉由不给出密钥进行攻击影响随机结果，进而选择他想要的受托人排序，这个排序有可能是为了下一轮更严重的攻击做准备。

我们可以将上述总结为收集分布式随机因子的随机性不足，因此需要洗牌以在收集的过程中引入随机性．洗牌让101位现任受托人参与了收集随机性的过程, 否则潜在的攻击可能会发生, 例如: [10]. 洗牌确保了每个受托人每回合只有一次发布的机会 (假设没有遗失区块)，因此他们无法透过引入新的密钥并预测新的受托人顺序来影响随机性，因为现在顺序是由上个回合的随机性所决定，而每个受托人只有一次机会来发布密钥。所有受托人发布的密钥会被用来做下一轮受托人顺序的洗牌之用，这表示在至少有一名受托人是诚实的情况之下，任何受托人无法串通来控制顺序。

4.4 解决“最后一个受托人作恶的问题”[11]

在DPOS 随机产生算法中, 作恶的受托人可以透过故意错过她负责产生的区块来抛弃不想要的随机结果. 这是他们唯一可以做的, 但是当随机过程的间隔小于一回合 (101个区块)时这会是一个潜在的问题, 因为作恶的受托人可以预测他将会在那个间格中产生哪个区块, 进而通过参与游戏可以确保在那个区块猜中结果赢得奖励。

我们可以将*BLOCK_TICKET_SALE* 定义为恶意受托人将会在一个区块内会买入的所有彩票.

如果出奖的间隔大于101个区块, 表示期间至少会有一次洗牌, 那么作恶受托人就无法预测他会分配到生产哪个区块. 那么他唯一的策略就是对进行猜测或是每个区块都参与. 如果是用猜的, 他的机会就是1/101, 而发动攻击的预期报酬就是他输掉的时候的彩票价格, 因为下一位受托人会继续取代他并随机出奖. 如果是每个回合都参与以达到至少猜中一次的目的, 他的攻击成本就是 (101 * *BLOCK_TICKET_SALE*), 但是预期的报酬仍然是他在单一区块的奖励汇报, 这样一来攻击的期望成本高于期望回报，从概率的角度来看是亏损的。

对于某些游戏来说, 101区块的出奖间隔太久, 因此需要快速猜测. 这时的方案如下, 出奖的结果可由两位受托人抽出:

第一位受托人的随机数只负责产生1到3之间的X, 以决定在他之后的第X个区块来的抽奖随机数. 第二位受托人可能是作恶并试图发动攻击, 但是他无法在四个区块之前预测谁会轮到产生抽奖随机数的区块, 因此他的攻击成本是 (3 * *BLOCK_TICKET_SALE*), 但是预期回报只有1 block_ticket_sale. 游戏规则唯一需要的就是设置第一个受托人一个区块之前的出奖间隔.

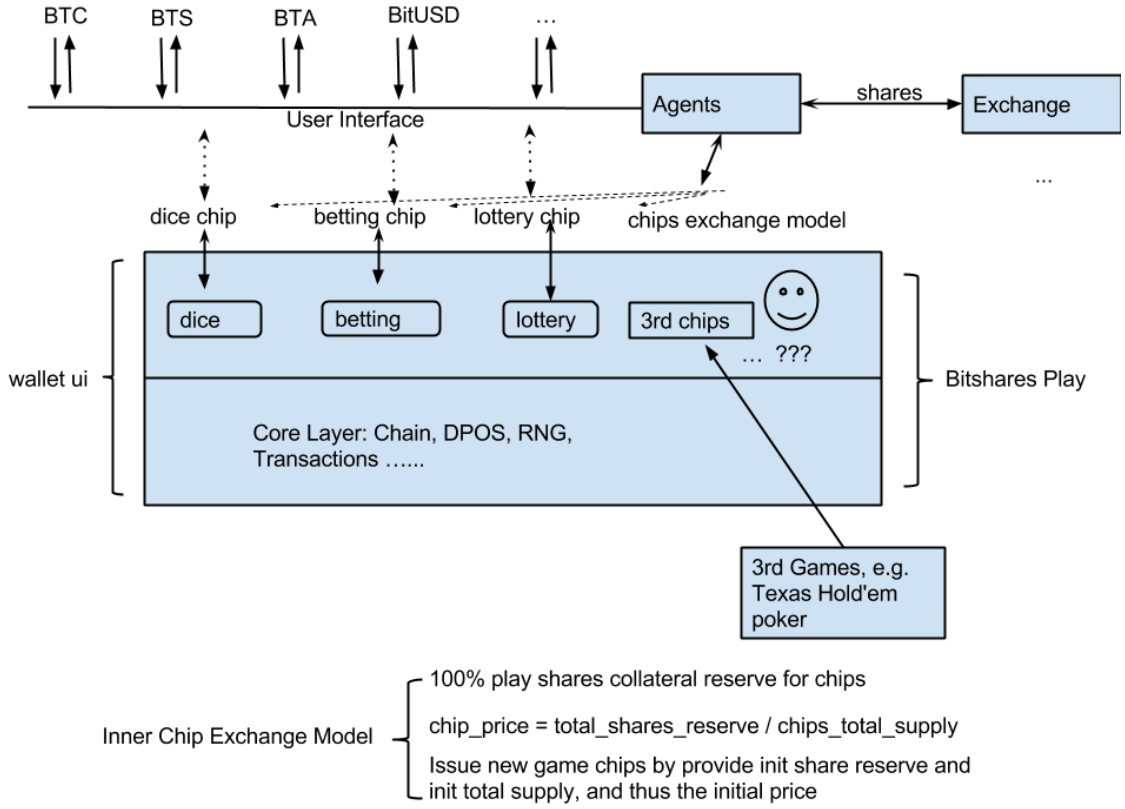
5.0 通往游戏平台和生态圈之路

5.1 规则层与核心层

比特股Play被设计成两个抽象层：规则层和核心层，这种设计可以很容易地将游戏集成与比特股Play资产模型分开来。在规则层，游戏开发者可以开发内置在比特股Play的游戏，或者在智能神谕（smart oracles）的帮助下集成第三方游戏的筹码资产，DPOS受托人在其中扮演着重要的角色。

核心层执行区块链和总账功能。规则层的设计会允许他人开发游戏，并能让不同的游戏币在经济上可达到平衡，同时又可以保持安全性和完整性。

游戏资产必须能安全地遵循它们与Play间的合约，它是不可信的，实际上还可能是恶意的。这是不同规则的代币（筹码）根据它们所抵押的PLS和他们当前的供应量，通过固定内场的价格来实现的。同时，市场用户可根据当前价格兑换游戏币，抵押或收回PLS。



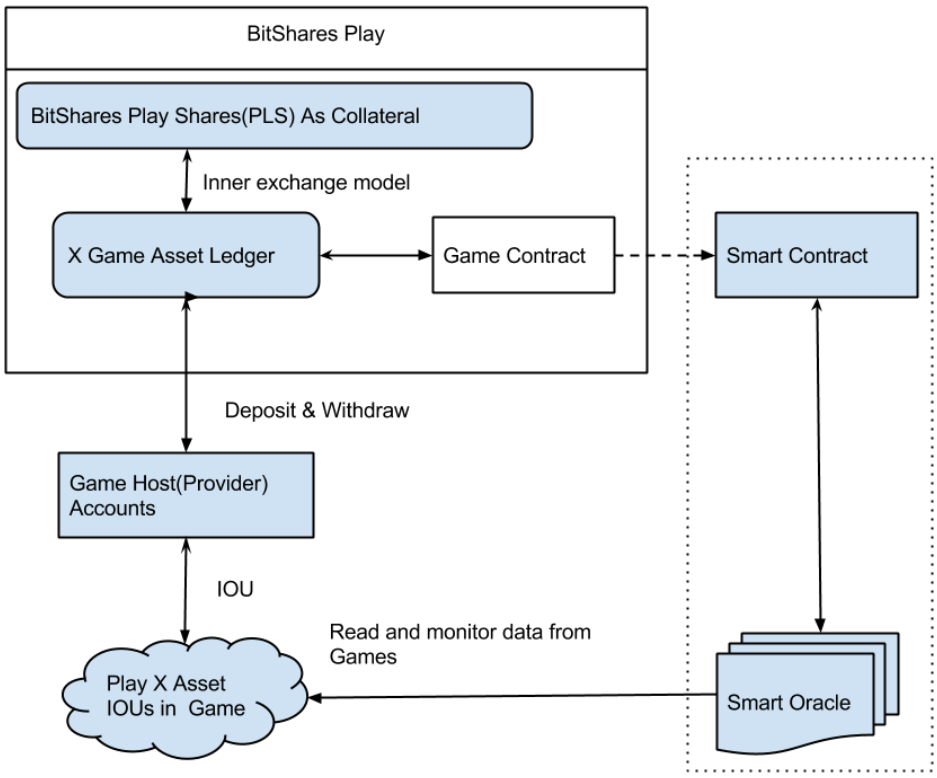
5.2 内置游戏作为系统的一部分

- 随机数生成。BitShares Play需要生成一个随机数，它可能会作为可靠的随机数直接用在游戏中。
- 游戏规则的定义。有许许多多的游戏规则，但他们的模型是类似的。实际上他们确实有非常多地方是共通的，以致它们可以被组合到一个抽象模型/层定义的规则。
- 我们需要一个映射方法来将幸运数和中奖号码连接成连续的自然数，以让我们可以将问题简化成自然数的随机生成。幸运数由用户根据某个规则模型选定。对于彩票的组合输入，我们可以借助数字组合系统（CNS）来实现。
- 精心设计的、拥有良好的经济平衡性的规则模型是非常有必要的，它可以使DAC保持自力持续。不应该出现由于奖励机制的缺陷而影响其他游戏的经济系统正常运行。
- 比特股Play的PLS市场不应该因为某个游戏币经济系统的不正常波动导致崩溃，例如某个游戏币的大量稀释和定向宽松导致游戏中奖者将得到的奖励全部抛向市场，默认的经济模型可以避免此类情况发生，此外还可以有很多其他措施作为建议提供给游戏开发者以避免游戏币本身的波动。
    - o 为了防止大量的中奖得主将他们（可能）得到的巨量游戏币抛向市场，奖金的分发应该被延迟，分布在多个区块中。这个机制应该属于交易验证中的一环，可以通过类似于比特币协议中的“nLockTime”来将支付在多个区块内进行锁定/冻结。BitShares Toolkit的交易信息中，有类似的参数：valid_until，可以用来实现这个功能。也就是说，如果一个输出是“奖励”输出，那它会被分成多个部分，每部分都有1至N个锁定时间，它们会在接下来的1至N个区块内发放。

5.3 与第三方游戏进行整合

传统游戏中的资产或点数无法提领来贩卖, 有些有外围市场的其实就是玩家储存在游戏商的欠条. 这些游戏资产没有抵押金来支撑, 并一般没有内建支持来存入获提领道其他的资产, 因此这样的市场没有流动性.

以下我们引入一种整合模式, 让游戏可以从比特股Play的游戏资产中获益.



游戏运营商不只是像是交易所地支持Play游戏资产的存入以及提领, 也提供了游戏软件以及服务。一个游戏对话是一种玩家以及游戏之间的半永久的交互式信息交换或对谈. 举例来说, 在过程中玩家可以买入游戏资产, 玩游戏, 以及在游戏之后提领资产。对于第三方游戏来说, 资产可能以游戏体验中的借条存在. 对于玩家来说, 要避免不良游戏主持商或是供货商最好的方式是在游戏之后提领游戏资产到Play当中. 游戏主持商可以透过像是merkle tree等技术证明他们的游戏资产存量. 但是这无法阻止游戏主持商在他们的游戏资产中创造不存在的资产. 藉由创造不存在的资产的作弊会在玩家无法从游戏主持商提领资产时暴露. 因此游戏主持商最好提供透明的API来让智能祭司监督以及审查。

这些智能祭司在连接DAC以及"真实世界"中扮演重要角色, 他们在DAC以及外部系统之间提供了一致的API, 包含了传统的中心化服务器. 假设总共有Y名智能祭司, 如果其中的X位对同一个输入传回了相同 (或一致)的输出结果, 那么我们就可以判断这个API呼叫是有效的. 这样一来, 我们就为DAC提供了一种健壮的去中心化方案, 并同时可以和"真实世界"互动。 DAC需要相信Y名智能祭司, 但是这个风险是很低的, 只要其中有X名没有串同, 结果就会是诚实的. 如果智能祭司是由Play持股人投票选出 (就像是DPOS的受托人一般), 这还可以再优化, 甚至可以让受托人直接担任智能祭司. 更多细节请阅读第六节的参考文献 [14].

第三方游戏本身就可以是DACs, 这样一来他的存入以及提领就会跟中心化的游戏略有不同. 此时DAC游戏内的资产就不在是风险较高的借据了. DACs和Play之间的存入以及提领可以透过系统的托管机制达成, 以在DAC之前能够跨链交换资产. 举例来说, 如果两个DACs A和B之间都支持这种机制, 那么就会有一个A-B的托管地址, 发到这里的币会在其中一个DAC中消失, 同时出现在另外一个DAC里面.

像是比特股X等系统拥有用户发行资产，可以作为某些数字实体的代币. 如果这样的系统支持了托管机制, 就可以在交易所内销毁一些比特资产 (例如PLS资产), 然后再创造相同数量的代币 (PLS)在比特股Play系统中, 反之亦然. 这当中可以透过两个系统之间的共识沟通达成，例如当Play侦测到某些数量的PLS资产送出到了托管地

址，然后相同数量的PLS就可以被创建在比特股Play系统中． 托管地址作为系统内的特殊地址，没有人知道私钥.

这样一来, DAC内的资产就可以互相操作. 这听起来就像是比特币的侧链机制以及双向锚定[15], 但是差异在于比特币侧链中只有一种代币 (比特币), 因此任何种类的托管都可能会造成稀释或是双重支付. 同时比特币侧链的机制也需要两条链的合并挖矿, 否则在采用POW的两条链之间, 算力较少的链可能会轻易地被较强的链上的算力51%攻击．如果两条链之间是锚定的, 那么他们就会需要被相同的算力所保护, 因此就需要融合挖矿. 但是这个问题并不适用于托管机制的系统, 因为每条链上面都有用户发行的资产来代表他们自己的链上的代币. 除此之外, 像是比特股X或是比特股Play的DPOS链上的股份都经由每个DAC的持股人所保护, 试图发动51%攻击就意味着想要变更系统托管共识的部分.

6.0 参考文献

[1] https://bitcoin.org/bitcoin.pdf
[2] http://en.wikipedia.org/wiki/Combinatorial_number_system
[3] http://bitshares.org/security/delegated-proof-of-stake/
[4] http://chancecoin.com/technical
[5] https://classic.satoshidice.com
[6] http://letstalkbitcoin.com/bitcoin-and-the-three-laws-of-robotics/
[7] http://trade.500.com/dlt/
[8] http://blog.bifubao.com/en/2014/03/16/proof-of-reserves/
[9] https://bitsharestalk.org/index.php?topic=4164.0
[10] https://bitsharestalk.org/index.php?topic=4009.msg59991#msg59991
[11] https://bitsharestalk.org/index.php?topic=6764.0
[12] http://www.random.org/randomness/
[13] https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/
[14] https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts
[15] http://www.coindesk.com/bitcoin-core-developers-bitcoin-side-chains/