Game Protocol: 一个创造新游戏的分布式经济体

GamyTech 团队

目录

1 任务

真钱竞技是一种游戏类型，在这种游戏中玩家根据自己的能力，而不是运气或机会来进行竞争而赢得真钱。GamyTech是一款多人真钱竞技游戏平台，可以让玩家在全球任何地方通过移动设备和个人电脑来与他人竞争。在成功向数百万用户发布了8款游戏后，GamyTech决定向公众开放我们的游戏平台，以便每个人都可以制作并发布自己的游戏。这将使GamyTech成为第一个开放式的游戏平台，其中 1）玩家可以享受大量的新游戏，2）游戏制作人可以根据自己的意愿创造新游戏，不必屈从于出版商的压力。

为此，我们计划开发“游戏协议”（Game Protocal，简称GP），一个首个基于区块链的游戏经济体，从而让拥有不同技能和资源的人们在开放的GamyTech平台上共同创造和体验新游戏。GP社区中的人们使用”游戏协议令牌”（Game Protocol Token，简称GPT），一种加密货币，按照彼此同意的条款于他人交换服务和资源。这种基于市场的交易机制构成了GP经济体的基础。GP经济体的参与者之间的特定交互模式（协议）将会被固化为智能合约以简化和自动化交换过程。

GPT将在所有主要的加密货币交易所上市。在一个健康的经济体中，人人协作以促进经济增长，并从增长中获益。通过在交易所交易GPT，GP经济体的贡献者可以获得经济上的奖励。

2 游戏协议服务

独立游戏制作人需要克服的第一个障碍是为他的新项目募集足够的资金。筹款一直是一个费时费钱的过程，但它是开发任何新游戏的先决条件。在GP经济体中，我们提供GameStarter，一个基于智能合约的全自动筹款系统，去帮助独立游戏制作人从筹款活动中获得最大收益。

在新游戏开发阶段，游戏制作人需要向开发人员支付报酬。其中一个主要问题是，直接进行链上支付的成本太高。为了解决这个问题，GP经济体提供了一个低成本的脱链支付渠道，这一渠道的成本比直接链上支付少很多。

促销是制作人完成新游戏后需要克服的另一个障碍。GP经济体提供了一种交叉营销服务，通过已经成功发布的游戏向现有的用户群来推广新游戏。

除了这三项服务之外，我们还提供了一个开发者工具，其中包含针对真钱竞争游戏的特定实用程序库。开发人员可以利用这些工具快速编写新游戏。

GamyTech在制作新游戏方面拥有丰富的经验。我们经历并成功克服了上述所有的痛点。在过去的三年中，我们筹集了超过300万美元的资金，并发布了8款新游戏。我们的游戏已经被下载超过400万次。我们现有的高级用户群（真正在游戏中花钱的用户）拥有约700,000名会员，他们在游戏中共赢得了约2,700万美元的奖金。

GP经济体所提供的服务和工具将极大的加强GamyTech平台的功能。通过利用这些服务，独立制作人可以确信，他们可以快速发布新游戏并直接访问GamyTech平台上的大量用户。

3 GameStarter

GameStarter是新游戏开发项目的一站式众筹平台。游戏制作人通过GameStarter发布新的“游戏专用筹码”（Game Specific Chip, 简称GSC）来资助他的项目。通过在GameStarter上集资，制作人可以在自己的全部视野下制作游戏，而不必屈从于出版商的压力，或处理基于法币的众筹平台中的各种繁文缛节。

投资者用本地货币GPT购买新游戏项目发行的GSC来投资。新的GSC的功能完全由游戏制作人自行决定：例如，GSC可以用于购买游戏中的特殊功能，提供对新游戏的完全访问权限，作为游戏中现金的替代品等等。

GameStarter筹款过程包括两个阶段：第一阶段，制作人向GameStarter提交一个合法的身份认证和一个白皮书。GameStarter将在公告板上发布该认证和白皮书以作为潜在的新项目提案，以便投资者检查和评估该提案。在第二阶段，GameStarter将自动生成一个智能合约，以便制作人管理和维护他的新GSC。

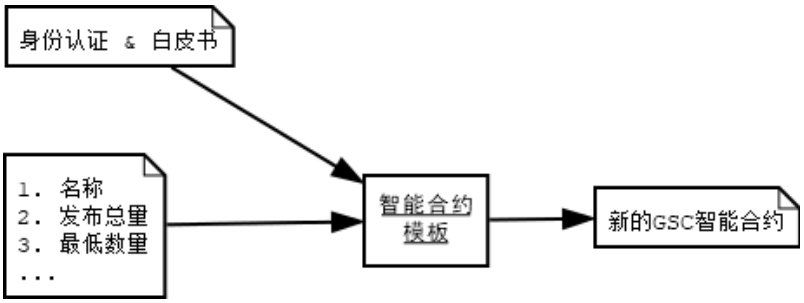

图 1: 生成GSC智能合约。

图1显示了生成新的GSC智能合约的过程。制作人在第一阶段提交的认证和白皮书将嵌

行号	输入	解释
1	名称	GSC名称
2	发布总量	GSC发布总量 (例如，1百万个GSC)
3	最低数量	筹款成功所需要的GPT数量(例如, 1000个GPT)
4	结束时间	筹款结束时间
5	GSC筹款价格	筹款中GSC的价格(例如， 0.5GPT/GSC)
6	制作人的账号地址	筹款成功后存放筹得GPT的账号地址
7	准备金率	智能合约在筹款结束后用来计算GSC的价格的一个输入(例如， 30%)

表 1: GSC智能合约输入。

入到生成的智能合约中并存储在区块链中。这确保GameStarter中的每个筹款活动的相关信息都可以被永久回溯。要生成新的智能合约，游戏制作人必须提供表1所示的信息。该信息与图1所示的智能合同模板结合生成最终的GSC智能合约。

生成的GSC智能合约要完成两项任务：1）在筹款活动期间管理资金，即接收投资者的GPT并为其分配GSC; 2）筹款活动结束后维护一个流动性池，任何人都可以向流动性池购买或出售GSC。

为了更好地理解生成的GSC智能合约如何实现这两种功能，我们需要首先描述GSC账本如何工作。

3.1 两个帐本的故事

如表2所示，每个GSC在区块链上都有自己的账本，就像本地货币GPT一样。然而，与GPT不同的是，GSC只能兑换GPT，而GPT可以在交易所兑换其他加密货币或法币，。此外，GSC不在任何交易所上市，它拥有自己的流动性池，任何人都可以通过流动性池买卖GSC。因此，GPT是GP经济体的储备货币，而每个新游戏项目都可以发行自己的，可以兑换成GPT的子货币GSC。

用GPT兑换GSC涉及两个帐本：GPT的帐本和GSC的帐本。举一个例子，假设账户“0x0cd2a”想要以0.5 GPT/GSC的价格从账户“0x227b”购买10个GSC。在这种情况下，我们需要将GPT从前者的账户转移到后者的GPT账户中，同时将10个GSC从后者账户转移到前者的GSC账户中。

GPT 账本	
...	...
0x0cd2a...	100 GPT
...	...
0x227b...	0 GPT
...	...

GSC 账本	
...	...
0x0cd2a...	0 GSC
...	...
0x227b...	1M GSC
...	...

表 2: GPT 和 GSC 账本.

由于每个账本分别由其各自的智能合约（分别为GPT智能合约和GSC智能合约）控制，因此这两个智能合约需要进行协调以完成这一双边交易。这种协调是通过将GSC智能合同注册成为GPT智能合同的“可信合同”来实现的。GPT合同包含一项特权功能：在账户之间转移GPT。只有受信任的合同才能访问此功能。显然，这可以防止黑客通过调用此特权功能来窃取GPT。

3.2 筹款活动

在筹款活动期间，所有筹得的GPT将存储在由GameStarter生成的一个辅助帐户中，新游戏的制作人无法控制该帐户。这样做是必要的，因为并非所有的筹款活动都会成功。如果筹款活动不成功，所有募集的GPT将由GameStarter退还给其所有者。如果成功了，那么筹得的总额将转移到制作人所控制的账户中（表1中的输入6）。

为了开展筹款活动，GSC智能合约首先使用自动生成的辅助帐户地址在GPT和GSC帐本上设置两个单独的帐户。 GPT账本中的账户将没有余额，因为尚未开始筹款，无人提供GPT; GSC账本中的账户保存了要发放的GSC的总量（表1中的输入2）。表2显示了具有辅助帐户地址“0x227b”的这两个账号。

投资者在GSC智能合约中调用函数“campaign_buy（address investor_address，uint GSCs_to_buy）”以购买GSC。该函数将首先调用GPT主合同来检查投资者是否拥有足够的GPT余额。如果他拥有，该函数将把指定数量的GSC从辅助账户转移到GSC账本上的投资者账户，然后它将调用GPT智能合约，从投资者账户中提取等量的GPT到辅助账户在GPT帐本的账号上。交换价格由新游戏的制作人指定（表1中的输入5）。

如果在筹款活动结束时间之前（表1中的输入4）筹得足够的，多余下限（表1中的输入3）的款项，则筹款活动成功。在这种情况下，函数“campaign_buy”将被禁用，即无法再从此

函数购买GSC。

3.3 流动性池

如果筹款活动成功，辅助帐户将被关闭。所有资产（包括筹得的GPT和剩余的GSC）将转移到新游戏制作人的账户中（表1中的输入6）。从那时起，制作人将完全控制了他拥有的所有资产。例如，他可以用GPT或GSC去支付为他的项目工作的程序员。与辅助账户一样，制作人的账户也有两个账号：一个在GPT账本上持有他筹集的GPT，另一个在GSC账本上持有剩余的GSC。两个条目都具有由新游戏制作人提供的相同的帐户地址。

制作人账户上的资产（GPT和GSC）构成了一个保留的流动性池，可以让任何人在任何时候使用从/向池中购买/出售GSC。 GSC的现货价格通过Bancor公式动态计算：

$$GSC\text{现货价格} = \frac{\text{流动性池中的}GPT\text{金额}}{\text{流通}GSC \times \text{准备金率}},$$

其中：

1. “流通GSC”是流通中的GSC总量（即发行的GSC总量（表1中的输入2）减去制作人账户中的GSC余额）;
2. “流动性池中的GPT金额”是制作人账户中GPT的总金额;
3. “准备金率”（表1中的输入7）是一个百分比，它代表流通中的GSC被GPT支持的百分比。

通过使用这个公式来确定GSC的现货价格，智能合同本质上是代表新游戏制作人为他发行的GSC做自动做市商。上述公式给出了交易无限小单位GSC的价格，要确定在购买交易中给定数量的GPT所能购买的GSC数量，或者出售交易中给定数量的GSC所能兑换的GPT数量，我们要用以下两个公式。有关详细信息，请参阅[1]

$$\text{购买的}GSC\text{数量} = \text{流通}GSC \times ((1 + \frac{\text{付出的}GPT\text{数量}}{\text{流动性池中的}GPT\text{金额}})^{\text{准备金率}} - 1),$$

[1] https://about.bancor.network/

$$\text{兑换的}GPT\text{数量} = \text{流动性池中的}GPT\text{金额} \times (1 - (1 - \frac{\text{出售的}GSC\text{数量}}{\text{流通}GSC})^{1/\text{准备金率}}).$$

4 脱链支付渠道

我们预计GP社区成员之间会有大量的直接支付交易。为降低交易成本，我们为GP社区建造一个脱链支付渠道。我们的目标是将成本降低到交易总额的一个小百分比（比如5％）。

为实现这一点，我们将交易记录批量的缓存到数据库中，直到批量达到特定阈值后再在在区块链上执行它们。对付款者来说，这意味着他们将无法立即收到现金。这对某些人来说可能并不合适，但他们随时可以选择直接在区块链上执行他们的交易（并支付相应的链上交易费用）。

想要利用我们的脱链支付渠道的用户首先需要在GamyTech中设置一个脱链支付账户。一旦完成，他需要向该账户提供一笔代币资金。只有在脱锁支付账户中持有的代币才能使用低成本的支付渠道。

每个脱锁账户的每笔付款都会记录到数据库中。从概念上讲，所有这些记录都可以组织成一个表格，如表3所示。每次发生新付款时，我们都会更新表格并检查是否有机会执行批次中的所有缓存交易。算法1显示该算法的概述。

	脱链支付账户余额	$user_1$	$user_2$	...	$user_i$	...
$user_1$	27.89	0	5	...	2.1	...
$user_2$	30	10	0	...	0	..
...	...	...	...	...	...	...
$user_i$	98.35	56	2	...	30	..
..	...	...	...	...	...	...

表 3: 存储的付账交易。

在算法1中，S_{ij}是从用户$user_i$到用户$user_j$的累计支付。在任何时候，S_{ij}或者 S_{ji}为零，或者两者同时为零，这是因为算法1总是结算任何一对用户之间的总支付量。这个结算程序是从第7行到第15行完成的。算法结束时，我们估算将所有缓存的交易在区块链中执行的总成本。如果此成本小于交易总额的一个百分比，我们将执行所有的交易。

Input : $user_i$ pays n tokens to $user_j$

if *$user_i$'s mircopayment account balance* $< n$ **then**
  trasaction fails;
else
  reduce $user_i$'s mircopayment account balance by n;
  let S_{ij} and S_{ji} be the values at cell ij and ji respectively;
  assert ($S_{ij} == 0$ or $S_{ji} == 0$);
  if $S_{ji} == 0$ **then**
    $S_{ij} = S_{ij} + n$;
  else
    if $S_{ji} \geq n$ **then**
      $S_{ji} = S_{ji} - n$;
    else
      $S_{ij} = n - S_{ji}$;
      $S_{ji} = 0$;
    end
  end
  let $a = \sum_{ij|S_{ij}>0} 1$, $b = \sum_{ij} S_{ij}$, $c =$ current average on-chain transaction cost, $d =$ current token value;
  if $\frac{ac}{bd} < 5\%$ **then**
    clear all cached transactions to the blockchain;
  else
    return;
  end
end

Algorithm 1: 脱链支付算法。

在实践中可以考虑这种算法的许多变种。例如，我们可以保证支付的时间而不是成本。为此，我们只需要定期执行缓存的交易。我们还可以将这两个标准混合使用：在特定时间段内尝试寻找低成本执行机会，并在截止日期过后执行缓存的交易。

5 交叉营销

交叉营销服务利用已经发布的游戏来推广新游戏。这类营销通常非常有效，因为营销针对的用户已经接触到已经发布的游戏。

交叉营销系统在服务器上为已经发布的游戏维护一个列表。新游戏可以以双方同意的价格从已经发布的游戏中购买这个列表的插槽。条款和价格完全由买卖双方决定，而且他们还可以选择低成本的脱链支付渠道进行付款。

每当用户开始玩已经发布的游戏时，服务器将以循环方式在插槽中选择新游戏广告，并向用户显示。图2显示了这样一个过程。插图中显示的Backgammon4Money是GamyTech最受欢迎的游戏之一。

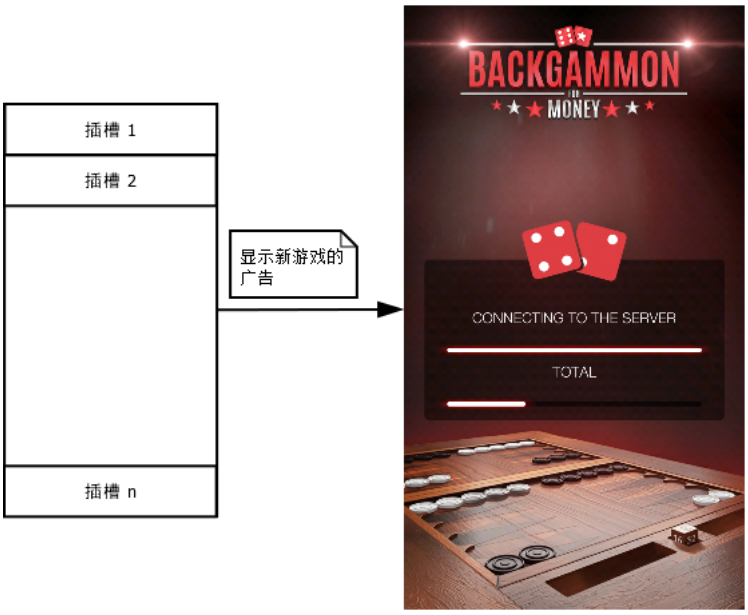

图 2: 交叉营销

由于真钱游戏始终需要连接到游戏服务器，因此每次在用户等待连接去重新开始游戏时，都是展示促销活动的绝佳时机。另一个显示广告的机会是游戏结束时。在游戏进行中展示任

何促销活动通常是不受欢迎的，这是因为对于正在争夺真钱的玩家来说，广告分散注意力。

鉴于我们拥有庞大而忠诚的用户群，我们预计交叉营销服务将成为对游戏制作商最具吸引力的GP经济体特征之一。

6 开发工具包

开发工具包含一组开发人员可以利用的工具来快速构建新的真钱游戏。这些工具经过精心设计，可解决真钱游戏中的常见问题，从而大大简化开发人员的工作。

具体来说，开发工具包提供以下功能：1）信用卡法币支付网关，2）保存玩家加密货币的加密钱包，3）投注智能合约，4）访问中央服务器的SDK ，以及5）公平的随机数发生器。

6.1 法币支付网关

我们的平台提供给游戏制作人的一个在游戏中接收法币支付的网关。维护这样的网关非常昂贵，因此独立游戏制作人通常没有这样的网关。通过在GamyTech平台上构建和发布新游戏，制作人可以通过我们提供的API访问此网关。

这项功能现已的部署就绪，我们目前使用它来为我们自己的游戏接受法币。

6.2 加密钱包

GP经济体支持的任何加密货币（包括ETH，GPT和由游戏发行的GSC）均可作为游戏中的令牌使用。为了支持这样的功能，我们为Unity游戏引擎开发了一个多币种加密钱包插件（下一步将为Unreal游戏引擎开发）。这个钱包可以安全地保存玩家的资产，并且还提供安全，明确的授权API来访问资产。具体而言，加密钱包支持以下功能：

1. 使用加密的密钥文件创建，导入和导出钱包;
2. 助记句和私钥恢复;
3. 在钱包之间直接转移代币;
4. 添加任何现有的智能合约在钱包中使用;
5. 使用合约职能和交易。

由于钱包与游戏引擎集成在一起，因此玩家可以在游戏中轻松使用代币（通过明确的用户授权），并从游戏中收集奖励。加密钱包是开源的，代码将被发布在GitHub上，以便开发人员检查并根据需要进行调整。

6.3 投注智能合约

投注智能合约的主要作用是作为一个可靠的第三方为玩家保存代币。在任何比赛开始之前，玩家将授权于投注合同去为他保存代币。在投注时，玩家所投金额应应少于为玩家所授权的的金额。

投注合同将包含3个将被服务器使用的功能。

1. 游戏开始 - 将接收玩家地址和一些游戏输入，比如游戏ID和赌注。该功能将从玩家转移令牌，直到游戏结束。如果转移任意一个玩家的令牌失败，其他玩家的赌注将被退还，游戏无法开始。

2. 游戏结束 - 将获得最终游戏状态（获胜玩家）。一旦比赛成功完成，投注智能合同将会转让下注的彩池给获胜玩家，并向收取费用。

3. 游戏取消 - 如果游戏遇到任何问题或错误，服务器将资金退还给所有玩家的钱包。

6.4 服务器SDK

我们为游戏开发者提供了一个访问中央服务器的SDK，以帮助他们开发游戏。此SDK使得开发者不用自己开发专用服务器去整合区块链。这将使游戏开发者能够充分专注于开发他们的游戏。

当游戏开始时，客户将使用加密钱包来确认他们的资金，以根据他们的余额知道他们可以参与哪些游戏匹配。钱包的资金被确认后，客户端将连接到服务器，并将传递钱包信息，以便服务器可以验证用户及其拥有的代币（通过区块链验证）。在成功验证之后，用户声明他愿意投注多少代币，并授权服务器从他的加密钱包中抽取此数量。此后，服务器将开始搜索具有相同所选赌注的匹配对手。一旦找到，服务器将从两个对手中抽取资金，存放到投注智能合约种，直到游戏结束，一方获胜为止。

由于转账需要一段时间，因此服务器不会等待转账资金到位，而会在等待时就开始比赛。如果其中某一次资金转账失败，比赛将被取消，资金将被退回。

6.5 随机数生成器

许多玩家所关心的一个问题是游戏中随机元素（例如骰子）的公平性。特别是如果他们输了，他们倾向于认为有人操控骰子。为了解决这个问题，我们构建了一个基于区块链的随机数生成器，它非常公平，任何游戏参与者都可以检查并证明没有人可以操纵游戏中生成的随机数。

一个简单的方法是使用区块链作为随机源。具体来说，这里是算法。

1 Each player i logins into the central server;
2 After registering all the players, the central server waits for K new blocks to be confirmed on the blockchain;
3 The central server uses the hash of the last confirmed block (i.e., the K-th block) as the seed to generate a random number in the gameplay;
4 Repeat the above steps if another random number is needed in the game;

Algorithm 2: 简单随机数生成器

有关算法2的一些说明：

1. 随机数发生器在中央游戏服务器上运行。

2. 每个人都可以确认并验证生成的随机数的种子由第K个区块的散列生成。

3. 由于没有人事先知道第K个区块的散列，所以这个算法是公平的。

4. 每次需要随机数字时，我们必须使用新的种子，以确保没有玩家可以模拟游戏。

5. 玩家必须等待一段时间才能开始玩游戏，因为服务器正在等待区块确认。

对算法2的一个担忧是区块链矿工可以控制以什么顺序生成哪些区块。虽然矿工能够以一种影响玩家获胜机会的方式来生成区块是极不可的，但我们仍然提供另一种算法来消除这个疑虑，如算法3所示。

关于这个算法的一些说明：

1. 由于每个玩家只有在其他人发布了hp_j后才上传自己的秘密号码p_i，他可以确定没有人能够与中央服务器勾结来操纵随机数发生器。

1 Each player i generates a private number p_i, calculates the hash of p_i as $hp_i = SHA3(p_i)$ and publishes hp_i to the blockchain;
2 Each player polls the blockchain. A player i sends the central server his private number p_i only after he has collected the hashes hp_j of all the other players;
3 After receiving p_i from a player i, the central server checks if $hp_i = SHA3(p_i)$. If not, abort and log player i as a bad actor;
4 After validating all p_i's, the central server calculates $p = \sum_i p_i$, and $hp = SHA3(p)$;
5 The central server uses hp as the seed and generates a random number for the gameplay;
6 Repeat the above steps if another random number is needed in the game;
7 After the game is over, the central server publish all private numbers received from all the players to the blockchain;

Algorithm 3: Random number generator version 2.

2. 中央服务器无法操纵随机数，因为种子hp是所有玩家共同决定的。

3. 新鲜的种子用于产生每一个随机数，玩家可以确定中央服务器不能以任何方式与对手勾结以增加后者的获胜机会。

这是一种昂贵的算法，因为参与者需要多次访问区块链来建立不可更改的记录以证明公平性。这是因为我们假设游戏参与者（包括玩家和中央服务器）都不相互信任。由于该算法仅将区块链用作共享信息的公共白板（而不是事务处理），因此我们可以使用免费和快速的区块链，如IOTA或Openchain。这将显着降低成本和等待时间。

7 令牌分发详情

只有150,000,000 GPT将被创建。不会有稀释，也不会产生跟多的令牌。58％的GPT将分发给公众。发行的GPT中有10％将保留在特殊的游戏支持基金中。该基金将允许该公司支持将在GameStarter上列出的有前途的游戏项目。该公司将保留指定他们将选择支持哪些游戏项目的能力。其余GPT中的20％将由公司保留（每6个月锁定25％）。表4显示了游戏协议的完整分发细节。

分发	数量	百分比
GPT总量	150,000,000	100%
共众分发	87,000,000	58%
游戏支持基金	15,000,000	10%
赏金计划	3,000,000	2%
顾问和合作伙伴	15,000,000	10%
公司(每6个月锁定 25%)	30,0000,000	20%

表 4: GPT 分发详情。

8 团队和顾问

有关所有团队成员和顾问的信息可以在以下网址找到：

http://gameprotocol.io