GameChain GC 游戏链白皮书

blockchain.game

GameChain GC 游戏链白皮书

Game Asset Transfer Protocol and DGAME Platform

创立新的游戏资产转移协议和去中心化游戏平台

基于区块链技术，变革传统游戏行业

由游戏行业资深专家，区块链行业资深专家，以及年轻富有创造力的技术，产品团队开发

目录：

第一部分：

概述

1. 摘要
2. 区块链的背景及意义

第二部分： 游戏链的设计原理及实现方法

3. 为什么设计游戏区块链
4. 区块链的目前技术难题和游戏链的解决方案
5. 游戏链的设计原则
    1. 与比特币相关协议的兼容性
    2. 支持百万级别用户
    3. 用户免费使用
    4. 模块化设计
    5. 低延时设计
    6. 安全可升级设计
    7. 产品和易用策略
6. 游戏链实现方案
    1. 游戏公共链
    2. 账户模型
    3. 智能合约和虚拟机
    4. 代币系统
    5. 共识模型

第三部分：游戏链的应用场景

7. 经济模型
8. 游戏相关的应用
9. 去中心化的游戏
10. 移动端的应用生态
11. 总结
12. 免责声明：
13. 参考文献：

版本记录：V0.3.2

第一部分：概述

1. 摘要：

GC 游戏区块链致力于开发构建在成熟区块链技术下的游戏区块链生态，为游戏用户及开发商提供成熟的游戏区块链架构体系，贡献游戏生态内容，打破现有的游戏行业规则，创造出新的商业模式。

在 GC 游戏链的白皮书中，我们详细描述了游戏链是怎样构思，设计，以及应用的。GC 游戏遵循良好的设计原则，参考了现有的区块链技术和生态，结合游戏行业的特点，我们提出多重技术和方式来结合游戏和区块链，解决现有游戏行业小团队盈利困难的问题，并且以提高区块链的性能，同时采取更多共识的方法，来拓展游戏区块链的应用范围。

区块链是一个全新的还在探索的行业，与游戏行业结合也有着无限的潜质，并且可以解决游戏行业中的一些痛点，在对于区块链框架和技术深入积累之后，我们重新设计了新的技术架构，并侧重于用最合适和经过验证的技术去搭建成熟的区块链产品。

2. 区块链的背景及意义

当中本聪在 2009 年 1 月启动比特币区块链时，他同时向世界引入了两种未经测试的革命性的新概念。第一种就是比特币（bitcoin），一种在没有任何资产担保、内在价值或者中心发行者的情况下维持着价值，去中心化的点对点的网上货币。目前为止，比特币已经吸引了大量的公众注意力，就政治方面而言，它是一种没有中央银行背书，并且有着剧烈的价格波动的货币。第二种就是共识机制：基于工作量证明的区块链概念。它使得人们可以就交易顺序达成共识。

作为应用的比特币可以被描述为一个先申请（first-to-file）系统：如果某人有 50BTC 并且同时向 A 和 B 发送这 50BTC，只有被首先确认的交易才会生效。没有固有方法可以决定两笔交易哪一笔先到，这个问题阻碍了去中心化数字货币的发展许多年。中本聪的区块链是第一个可靠的去中心化解决办法。现在，开发者们的注意力开始迅速地转向比特币技术的下一章节，区块链怎样应用于货币以外的领域。但由于比特币缺乏图灵完备性，并不能实现循环等逻辑，所以比特币并不适合于开发其他应用场景，Vitalik 在 2013 年发布新的白皮书提出一种图灵完备的区块链体系“以太坊”，提出以构建 Web3.0 让区块链成为新的互联网 3.0 的思路，才使得区块链真正在应用领域有广泛的应用价值。

以太坊是一个带图灵完备的“智能合约“区块链，智能合约用简单的逻辑表述，即这是一套根据事先任意制订的规则来自动转移数字资产的系统。例如，一个人可能有一个存储合约，形式为“A 可以每天最多提现 X 个币，B 每天最多 Y 个，A 和 B 一起可以随意提取，A 可以停掉 B 的提现权”。这种合约的符合逻辑的社会化场景就是去中心化自治组织 DAOs（Decentralized Anonymous Organizations）使用的一个长期的包含一个组织的资产并把组织的规则编码的智能合约。以太坊的目标就是提供一个带有内置的成熟的图灵完备语言的区块链，用这种语言可以创建合约来编码任意状态转换功能，用户只要简单地用几行代码来实现逻辑，就能够创建以上提及的所有系统以及许多我们还可能想象不到的的其它系统。

然而在游戏领域，基于比特币和以太坊的区块链网络结构可能并不合适，原因是目前比特币以太坊只能够提供少量 TPS，会造成一定的拥堵，严重影响到游戏产业

的运营，另外以太坊的生态系统并不够完善，在底层设计上缺乏一定的权限限制。我们思考过用两种方式构建新的游戏链，1.在以太坊上构建游戏侧链的生态。2.自己重建专属领域新的区块链。经过一段时间的技术实验和测试，在严谨考察了共识，生态，性能几方面后，我们决定重新设计基于 DPOS 的共识机制。我们考虑到基于 POW 的共识机制是目前最有效的共识方法，但是这并不是完美性能的解决方案，基于 DPOS 的共识机制在性能上能够解决问题，但是弱在不能完整的去中心化，我们决定取一个折衷的方案。

第二部分： 游戏链的设计原理及实现方法

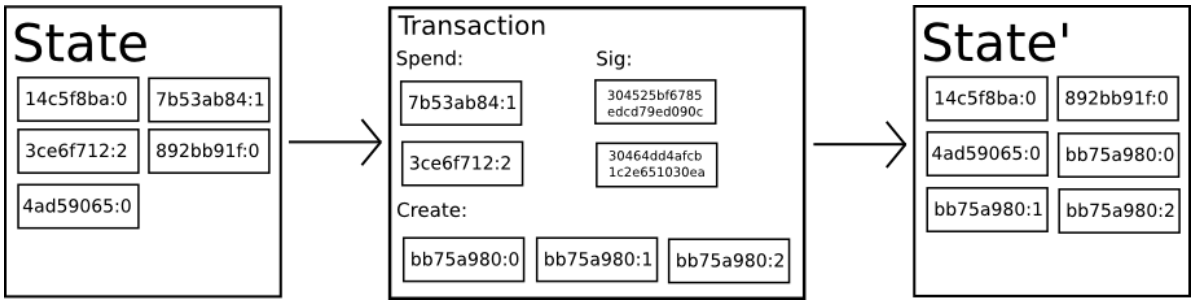
3. 为什么设计游戏公有链

游戏行业但巨头林立，存在各种风险，包括行业风险，市场风险，核心人员流失的风险，财务风险等等。用去中心化的公司方式去制作游戏，可能可以解决游戏行业的这些问题，但是现有的区块链平台平台被高额交易费用和受限制的计算能力限制，并不适合游戏行业使用。因此我们针对以上这些风险和痛点，设计并研发游戏链。

4. 区块链的目前技术详解和游戏链的解决方案

自中本聪设计的比特币开放源代码以来，比特币已经运行了 8 年，比特币是第一个基于 POW 的共识的公共账簿的应用。我们先来看一下比特币系统的原理：比特币是一个将基于节点的去中心化共识协议与工作量证明机制结合在一起的账簿系统。在系统中，节点通过工作量证明机制获得参与到系统的权利，每十分钟将交易打包到“区块”中，从而创建出不断增长的区块链。在这个系统中，拥有大量算力的节点有更大的影响力。从而形成一个非常庞大的算力网络，想获得比整个网络更多的算力比创建一百万个节点困难得多，这些算力维护着比特币系统的稳定性。尽管比特币区块链模型非常简陋，但是实践证明它已经足够好用了，在未来五年，它将成为全世界两百个以上的货币和协议的基石。

作为状态转换系统的比特币



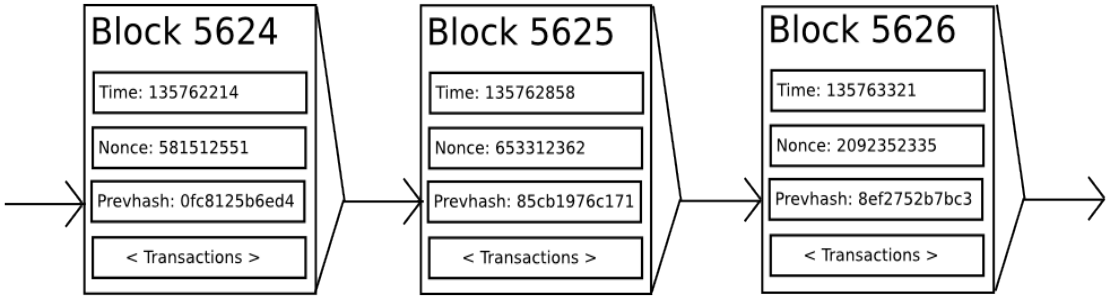
从技术角度讲，比特币账本可以被认为是一个状态转换系统，该系统包括所有现存的比特币所有权状态和“状态转换函数”。状态转换函数以当前状态和交易为输入，输出新的状态。

例如，在标准的银行系统中，状态就是一个资产负债表，一个从 A 账户向 B 账户转账 X 美元的请求是一笔交易，状态转换函数将从 A 账户中减去 X 美元，向 B 账户增加 X 美元。如果 A 账户的余额小于 X 美元，状态转换函数就会返回错误提示。
所以我们可以如下定义状态转换函数：
APPLY(S,TX) > S' or ERROR

在上面提到的银行系统中，状态转换函数如下：
APPLY({ Alice: $50, Bob: $50 },"send $20 from Alice to Bob") = { Alice: $30,Bob: $70 }
但是：
APPLY({ Alice: $50, Bob: $50 },"send $70 from Alice to Bob") = ERROR

比特币系统的“状态”是所有已经被挖出的、没有花费的比特币（技术上称为“未花费的交易输出，unspent transaction outputs 或 UTXO”）的集合。每个 UTXO 都有一个面值和所有者（由 20 个字节的本质上是密码学公钥的地址所定义）。一笔交易包括一个或多个输入和一个或多个输出。每个输入包含一个对现有 UTXO 的引用和由与所有者地址相对应的私钥创建的密码学签名。每个输出包含一个新的加入到状态中的 UTXO。在比特币系统中，状态转换函数 APPLY(S,TX)->S’大体上可以如下定义：
交易的每个输入：
如果引用的 UTXO 不存在于现在的状态中（S），返回错误提示
如果签名与 UTXO 所有者的签名不一致，返回错误提示
如果所有的 UTXO 输入面值总额小于所有的 UTXO 输出面值总额，返回错误提示
返回新状态 S’,新状态 S 中移除了所有的输入 UTXO，增加了所有的输出 UTXO。

第一步的第一部分防止交易的发送者花费不存在的比特币，第二部分防止交易的发送者花费其他人的比特币。第二步确保价值守恒。比特币的支付协议如下。假设 Alice 想给 Bob 发送 11.7BTC。事实上，Alice 不可能正好有 11.7BTC。假设，她能得到的最小数额比特币的方式是：6+4+2=12。所以，她可以创建一笔有 3 个输入，2 个输出的交易。第一个输出的面值是 11.7BTC，所有者是 Bob（Bob 的比特币地址），第二个输出的面值是 0.3BTC，所有者是 Alice 自己，也就是找零。
我们再来看一下生成新区块的挖矿模式



每一个区块，每个区块包含一个时间戳、一个随机数、一个对上一个区块的引用（即哈希）和上一区块生成以来发生的所有交易列表。这样随着时间流逝就创建出了一个持续增长的区块链，它不断地更新，从而能够代表比特币账本的最新状态。
依照这个范式，检查一个区块是否有效的算法如下：
检查区块引用的上一个区块是否存在且有效。
检查区块的时间戳是否晚于以前的区块的时间戳，而且早于未来 2 小时[2]。
检查区块的工作量证明是否有效。
将上一个区块的最终状态赋于 S[0]。

假设 TX 是区块的交易列表，包含 n 笔交易。对于属于 0……n-1 的所有 i,进行状态转换 S[i+1] = APPLY(S[i],TX[i])。如果任何一笔交易 i 在状态转换中出错，退出程序，返回错误。返回正确，状态 S[n]是这一区块的最终状态。

本质上，区块中的每笔交易必须提供一个正确的状态转换，要注意的是，“状态”并不是编码到区块的。它纯粹只是被校验节点记住的抽象概念，对于任意区块都可以从创世状态开始，按顺序加上每一个区块的每一笔交易，（妥妥地）计算出当前的状态。另外，需要注意矿工将交易收录进区块的顺序。如果一个区块中有 A、B 两笔

交易，B 花费的是 A 创建的 UTXO，如果 A 在 B 以前，这个区块是有效的，否则，这个区块是无效的。

区块验证算法的有趣部分是“工作量证明”概念：对每个区块进行 SHA256 哈希处理，将得到的哈希视为长度为 256 比特的数值，该数值必须小于不断动态调整的目标数值，本书写作时目标数值大约是 2^190。工作量证明的目的是使区块的创建变得困难，从而阻止女巫攻击者恶意重新生成区块链。因为 SHA256 是完全不可预测的伪随机函数，创建有效区块的唯一方法就是简单地不断试错，不断地增加随机数的数值，查看新的哈希数值是否小于目标数值。如果当前的目标数值是 2^192，就意味着平均需要尝试 2^64 次才能生成有效的区块。一般而言，比特币网络每隔 2016 个区块重新设定目标数值，保证平均每十分钟生成一个区块。为了对矿工的计算工作进行奖励，每一个成功生成区块的矿工有权在区块中包含一笔凭空发给他们自己 25BTC 的交易。另外，如果交易的输入大于输出，差额部分就作为“交易费用”付给矿工。顺便提一下，对矿工的奖励是比特币发行的唯一机制，创世状态中并没有比特币。

为了更好地理解挖矿的目的，让我们分析比特币网络出现恶意攻击者时会发生什么。因为比特币的密码学基础是非常安全的，所以攻击者会选择攻击没有被密码学直接保护的部分：交易顺序。攻击者的策略非常简单：

向卖家发送 100BTC 购买商品（尤其是无需邮寄的电子商品）。

等待直至商品发出。

创建另一笔交易，将相同的 100BTC 发送给自己的账户。

使比特币网络相信发送给自己账户的交易是最先发出的。

一旦步骤（1）发生，几分钟后矿工将把这笔交易打包到区块，假设是第 270000 个区块。大约一个小时以后，在此区块后面将会有五个区块，每个区块间接地指向这笔交易，从而确认这笔交易。这时卖家收到货款，并向买家发货。因为我们假设这是数字商品，攻击者可以即时收到货。现在，攻击者创建另一笔交易，将相同的 100BTC 发送到自己的账户。如果攻击者只是向全网广播这一消息，这一笔交易不会被处理。矿工会运行状态转换函数 APPLY(S,TX)，发现这笔交易将花费已经不在状态中的 UTXO。所以，攻击者会对区块链进行分叉，将第 269999 个区块作为父区块重新生成第 270000 个区块，在此区块中用新的交易取代旧的交易。因为区块数据是不同的，这要求重新进行工作量证明。另外，因为攻击者生成的新的第 270000 个区块有不同的哈希，所以原来的第 270001 到第 270005 的区块不指向它，因此原有的区块链和攻击者的新区块是完全分离的。在发生区块链分叉时，区块链长的分支被认为是诚实的区块链，合法的的矿工将会沿着原有的第 270005 区块后挖矿，只有攻击者一人在新的第 270000 区块后挖矿。攻击者为了使得他的区块链最长，他需要拥有比除了他以外的全网更多的算力来追赶（即 51%攻击）。

以太坊目前也是用 POW 机制实现，目前在基于 POW 的系统看来，比特币和以太坊的 TPS 存在严重不足，以太坊网络曾经发生大规模拥堵，原因是使用以上的 POW 机制并不能够支撑稍微大型的网络执行速度，也不能实现秒级验证机制。

所以，在这里我们引入 BTS 的 DPOS 机制，我们先深入了解 DPOS 的原理：在比特币网络产生一个区块的时间过后，一个授权股权证明系统(DPOS)能使你 的交易得到 20%股东的核实，而在比特币网络声明交易已几乎不可逆(6 个区块， 约 1 小时)的时间过后，在 DPOS 机制下，通过其代表，你的交易已经得到 100% 股东的核实。当使用去中心化自治公司(Decentralized Autonomous Company, DAC)这 一说法时，去中心化表示每个股东按其持股比例拥有影响力，51%股东投票的结 果将是不可逆且有约束力的。其挑战是通过及时而高效的方法达到 51%批准。为达到这个目标，每个股东可以将其投票权授予一名代表。获票数最多的前 100 位代表按既定时间表轮流产生区块。每名代表分配到一个时间段来生产区块。 所有的代表将收到等同于一个平均水平

的区块所含交易费的 10%作为报酬。如果 一个平均水平的区块含有 100 股作为交易费，一名代表将获得 1 股作为报酬。

在分叉处理中，网络延迟有可能使某些代表没能及时广播他们的区块，而这将导致区块链分叉。但是，这不太可能发生，因为制造区块的代表可以与制造前后区块的代表建 立直接连接。建立这种与你之后的代表(也许也包括其后的那名代表)的直接连接 是为了确保你能得到报酬。

该模式可以每 30 秒产生一个新区块，并且在正常的网络条件下区块链分叉 的可能性极其小，即使发生也可以在几分钟内得到解决。针对代表的分布式拒绝服务攻击(DDOS)，发生后因为只有 100 名代表， 可以想象一个攻击者对每名轮到生产区块的代表依次进行拒绝服务攻击。幸运的是，由于事实上每名代表的标识是其公钥而非 IP 地址，这种特定攻击的威胁很容易被减轻。这将使确定 DDOS 攻击目标更为困难。而代表之间的潜在直接连接，将使妨碍他们生产区块变得更为困难。

基于 DPOS 的共识机制可以有效地改善区块链网络吞吐性能。可以使得网络承载更多的交易。游戏行业是需要一个高吞吐量，性能敏感的行业，所以这样的共识模型更适用于游戏链。

5. GC 游戏链的设计原则：

与比特币相关协议的兼容性。

比特币网络的生态系统是目前最大的一个区块链技术的生态系统，根据网络效应和马太 效应（Matthew Effect）的影响，我们有理由相信比特币生态系统会进一步扩大和完善， 也意味着更高的代码成熟度和更多的开发者。我们游戏链在设计的时候，尽量保持与比特币和以太坊系统的兼容性，这样以后借力社区的宝贵经验，使用比特币的相关协议，提供了技术上的可能性。因此游戏链后面可以兼容大部分的比特币以太坊的协议，例如闪电网络（lighting network）和侧链（sidechain）和驱动链技术(drivechain) 和基于零知识证明的 Zcash 协议等。

支持百万级别用户

现有游戏应用需要极高的响应速度，另外游戏有大量的用户，这个需要区块链的技术方案可以承载大量数百万的日常活跃用户，在一些情况下，如果用户量过少，游戏程序可能不会运营。所以支持数百万级别以上的用户是必须的，这样才有商用价值。

用户免费使用

游戏开发者需要提供一定免费的服务，如果在使用之前需要在区块链中付费，这个是不合适的，一个对用户来说可以广泛使用的区块链平台可以获的更大范围的去中心化，开发者可以获得更有效的盈利策略

模块化设计

为了可维护性，我们将充分解耦各个功能模块区块链层，智能合约虚拟机层，API 层，应用 SDK 层。在核心区块链功能我们开放给社区维护，采用 MIT 协议。

低延时设计

良好的用户体验需要可靠的用户反馈以及比较低的延时，长时间的延时会让用户觉得使用区块链支持的游戏不如不用区块链设计的游戏。我们设计的秒级确认模式，可以保证良好的用户体验。

安全可升级设计

为游戏应用而设计的区块链，基础的设计需要灵活性和可升级性，任何的软件都会有 bug，区块链的设计也如此，平台必须足够健壮，能够快速修复各种新出现的 bug，我们设计的 GVM 虚拟机有授权机制，为了防止 DDOS 攻击和网络阻塞，一般节点是不支持智能合约的运行，智能合约运行需要区块链网络资源开销，只有经过授权的节点可以。

产品和易用策略

区块链产品是一个极其重要的策略，目前区块链应用有不易理解，难以使用等缺陷。易用作为游戏链的核心优势之一，也是更大范围去中心化的保障方式。

6. 游戏链实现方案

(1). 游戏链公链

Bitcoin 和 Ethereum 都通过去中心化建立了一条公链，GC 游戏链目的是建立一条去中心化游戏领域的公共链，通过高性能和策略机制确保整个网络无阻塞，实现资产的点对点流动。

(2). 账户模型

游戏链中可自由新建账号，基于人类可识别的账户模型，由一个可以识别的代号便于清晰的确认账户地址和账户名称。同时可以设置命名空间，可以进行组织分层。

(3). 智能合约和虚拟机

以太坊的 EVM 是目前广泛测试的唯一的区块链虚拟机，在可以预见的未来，EVM 将会成为重要的区块链虚拟机体系，Solidity 开拓性地定义了基于区块链的语言应该呈现的形态。除此之外 Javascript 拥有快捷灵活的语言体系，ES2015 更是奠定了 javascript 在互联网行业的重要地位，我们 GVM(Gamechain Virtual Machine)设计可扩展语言模块，可兼容以太坊的 EVM，采用 Solidity，同时支持 Javascript，以兼容各种设计模式和语言习惯。

(4). 代币系统

GameCoin 为游戏链指定代币，也作为执行智能合约的支付工具，并且作为去中心化游戏项目的众筹货币，网络包含自身的内置货币 GC，并扮演双重角色，为各种数字资产交易提供主要的流动性，更重要的是提供了了支付交易费用的一种机制。

(5). 共识模型

在游戏链的共识机制的选取中，根据共识的可靠性原则和去中心化原则，我们最终选取 DPOS 为基础的共识机制作为公链的基础共识机制。之前社区对共识机制的讨论较多，从 POW 到 POS 到 DPOS， 再 到 HyperLedger 提出的 BFT 共识机制。共识机制的本质在于在一个分布式系统中如何通过一些算法，最后取得数据的一致性。关于共识机制的讨论最后都会回归到计算机领域的分布式系统的一致性问题，之前这个领

域已经有很多的研究和成果，例如分布式系统中的 FLP 定理和 CAP 定理指导人们如何根据具体的需求来设计共识机制。我们采用的 DPOS，融合 TPOS 机制.

POW 机制

在比特币的网络中，矿工通过比特币的全客户端一起参与到比特币网络的校验过程，通过工作量证明的方式，来随机碰撞 Hash 值，当矿工计算 Hash 值，满足一定条件时，我们就说该矿工挖到了一个区块。也即 Hash(A) < M/D- Hash 函数代表 2 次的 SHA256 计算，取值范围是[0, M]，D 是[1, M]的一个整数，比特币网络的 SHA256 挖矿算法可以让每一个节点快速验证区块的有效性，并且 BlockHeader 每一个区块都随着 Nonce 和 extra Nonce 的不同而改变。整体挖矿的难度会根据网络的总算力而动态调整，根据共识协议，让网络有分叉产生的时候，我们会选取包含更多工作量的区块作为有效的区块。后面根据挖矿算法的不同，还产生了其他的 Proof of Work 的算法，例如 Litecoin 的 Script 算法，Darkcoin 的 X11 算法，设计的初衷是抵制算力集中化，从而保证网络的去中心化。然而 POW 机制受到大量性能制约，并不适用于性能密集型产业。

DPOS 机制

GC 游戏链优化了共识模型，在参考区块链现有的共识模型的基础上，我们优化了 DPOS（Delegated Proof of Stake）算法，在此算法下，拥有代币的用户通过持续的赞同投票系统，可以选择生成新区块的生成者。这些参与生成新区块的人将会有机会生成对应份额的新区块。游戏链的区块生成速度为 3 秒，在 3 秒之内，只有一个可以生成新区块的区块生成者，如果新的区块在既定的时间内没有被生成，这个区块将会被跳过，如果有一个区块或更多的区块被跳过，将会有 6 个或者更多的区块间隔。使用游戏链的区块生成模型，每个区块在 21 个轮回中循环，在每个 21 轮以后，独立的区块生成着将被生成，排在前排的 20 个被确认的将会自动被每一轮选择然后最后一个生成者按照比例生成，这些被选定的生成着使用一个由区块时间决定的伪随机算法，这个随机生成算法将会确定所有的生成着维护一个和其他生成着一样平衡的链接性，如果一个生成着错过一个区块，然后在近 24 小时之内并没有生成任何新的区块，他将会被移出队列，一直到他重新链接区块链，并通知区块链我可以重新生成区块，这种方式通过最小化那些被证明不可靠的错过的区块，确保网络平滑的运作。在正常情况下，1 个 DPOS 区块链不会发生分叉，因为区块生成者不是通过竞争生成而是通过合作生成，一但发生分叉，共识将会自动切换到最长的区块链上。在这种情况下双花也不会出现。

交易确认

典型的 DPOS 区块链是有 100%的区块参与，一笔交易一旦倍 99.9%的确认，即被确认。也会有一些特别的情况，一但区块链软件 bug 出现，或者网络阻塞，或者恶意的区块生成者将会创造两个分叉，一个节点必须等待 21 个区块中的 15 个的确认，机遇一个典型的配置，这个将会花费平均 45 秒钟的正常等待时间。默认情况下，所有节点都会确定在 21 个中 15 个不可以撤回。而且将不会切换到那个分叉的区块。

TPOS（Transaction as Proof of Stake）算法

游戏链的每一笔转账都需要包括前一个区块的前一个区块头，这一段哈希有两个目的：

1.防止在分叉分支的重放攻击

2.标示哪个网络是在分叉的地方

7. 系统模型

账户模型

游戏是一个强账户形式的生态，账户对于人可读的，名称是由创建者决定的，所有的账户的建立是需要收费的，同时账户也支持命名空间，在去中心化的内容中，游戏设计者将会提供创建账户所需要的开销。创建之后，就不需要在另外的游戏中注册。

经济模型：

在经济系统中，我们设计了 GC 货币模式，游戏股权模式，游戏金币模式，等三种代币，游戏资产有，游戏账号，游戏道具，游戏金币，游戏周边资产有视频，游戏分享等模式，游戏模式中有竞技场，竞赛模式，点对点竞技，团队竞技，生态有矿业生态，对战生态，视频分享生态等，游戏团队在链上可以发行资产，为游戏带来新的商业模式。
GC Token 为指定代币。

8. 游戏相关的应用：

面向移动端策略是推动游戏区块链，技术落地的一个重要环节，在游戏链的生态系统中，我们不仅全面支持并推动移动应用战略，而且我们将会与第三方开发者，一起为用户提供移动端的服务，包括：移动端钱包、移动端 DGAME 应用、移动端智能合约应用等服务。我们也鼓励第三方的开发者，加入我们，一起推动区块链技术在中国的落地，开发出普通用户可以使用的区块链移动端服务。

区块链基础工具

区块链基础工具是指 GC、钱包、账号系统这样的必需组件。他们将可复用的组件模块化，这些组件可以用作应用的基础，且可以得到改进。

身份系统

每个账户都会有一个指定的、独一无二的 ID.用户可以注册独一无二的名称，并将名称与一 个数据结构的 Merkle 根相连。数据结构可包含一个用户的独一 ID 和其它账户信息。我们预 计将使用 JSON 格式来代表诸如个人或公司这样的实体。

钱包

钱包是一个用来与 GC Token 发生互动的软件。钱包将掌管 GC 私钥，并创建和签署交易。 用户可以使用钱包来发送通道交易，并使用连接网络的 app.

收费 API

今天的绝大多数 API 都是公开的，任何人都可以调用，又或者调用某些 API 需要用户名-密码 或特有访问代币。支付通道使得一种新型 API 变得可能，人们可以为每一次的 API 调用付费， 甚至是每一次 HTTP 请求。支付以访问 API 还解决了 DDoS 问题，且使得建设高质量的、总 是可用的 API 变得更便捷。需要支付的 API 响应是创建一些至今尚不可能的商业模型的基础 需求，可以在未来的去中心化经济中扮演非常重要的

角色。他们可以为信息的持有人提供经 济激励，让他们将原本私有的数据变得公开可用。

保险系统

新创建娱乐保险系统，防止沉溺。作为新的一种财产保障体系。

安全众筹

我们可以使用优先保障合约(dominant assurance contracts)来部署安全的众筹活动。

点对点通讯系统

使用区块链级别的安全加密技术，目前无法破解。方便私密通讯，解决隐私问题，解决监听和网络传输问题。

隐私保护

游戏链系统将通过智能合约管理平台的上的用户。系统将提供可选的身份识别模块，是区块链系统可以对接金融系统的前提条件。系统开发者将开发基于相应的智能合约代码，并可以链接第三方机构，同时也可以生成匿名玩家，只使用匿名的用户系统。

9. 去中心化游戏应用（DGAME）

游戏链系统致力从技术层面全面支持去中心化应用，尤其是通过移动端策略的引入，将不同的 DGAME 想法产品化，可以把区块链技术带给更多的游戏用户和行业。例如去中心化的社交、去中心化的存储和去中心化的游戏域名服务、去中心化的分享服务等，通过激励机制的引入，将更深层次利用共享经济的理念，改变现有的游戏市场和商业模式。

游戏链区块链技术为搭建去中心化应用（Decentralized Game)提供基础架构。在游戏链中，通过完善的 API 的设计和 Docker 的分发，简化开发者的准备工作，使开发者可以快速上手相应的开发工作。并将通过游戏链系统内部的 Token 激励开发者开发出高质量的 DGAME。

在游戏链系统中，可以支持多种游戏的应用需求：例如游戏中的金融业、社交和股权等。另外基于游戏链的智能合约，通过图灵完备的编程语言，可以实现更复杂游戏资产的流动的。

10. 移动端的应用生态

移动端应用是技术落地的一个重要环节，在游戏链的生态系统中，我们不仅全面支持并推动移动应用战略，而且我们将会与第三方开发者，一起为用户提供移动端的服务，包括：移动端钱包、移动端 DGAME 应用、移动端智能合约、移动视频直播等应用等服务。我们也鼓励第三方的开发者，加入我们，一起推动区块链技术在中国的落地，开发出普通用户可以使用的区块链移动端服务。区块链移动应用的核心问题是节点过重，对于移动计算来说，轻量可快速确认的应用更加适合用户，我们因此设计了

外围节点，我们称他为 Moon 节点，Moon 节点 环绕 Earth 节点工作，提供基础的移动应用支持。

11. 总结：

游戏链是一条区块链公共链，其核心目标是构建一个高性能去中心化安全稳定的承载区块链游戏资产的支撑平台。

未来展望：我们希望通过构建游戏区块链，真正创造出去中心化的游戏应用，来拯救现有游戏的生态。为区块链和游戏行业带来更多的解决方案。

12. 免责声明：

区块链作为新兴产业，具有极高的投资风险和技术风险，属于高风险投资行业。白皮书作为技术和产品描述，描述了技术和产业的布局和前景，不建议没有风险承受能力的人进行投资。

13. 参考文献：

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/ bitcoin.pdf. Oct 2008

[2] Vitalik Buterin. Ethereum White Paper : A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/ wiki/White-Paper.

[3] Wikipedia. Directed acyclic graph. https://en.wikipedia.org/wiki/Directed_acyclic_graph.

[4] Serguei Popov for Jinn Labs. The tangle. https://iota.org/IOTA_Whitepaper.pdf, April 2016.

[5] Anton Churyumov. Byteball: A Decentralized System for Storage and Transfer of Value. https://byteball.org/Byteball.pdf,September2016.

[6] Wikipedia. PoW. https://en.wikipedia.org/wiki/Proof-of-work_system.

[7] Wikipedia. PoS. https://en.wikipedia.org/wiki/Proof-of-stake.

[8] "Nxt Whitepaper (Blocks)". nxtwiki. Retrieved 2 January 2015.

[9] mthcl (pseudonymous). "The math of Nxt forging" (PDF). pdf on docdroid.net. Retrieved 22 December 2014.

[10] Ori Brafman. The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations. 2006.

[11] Yochai Benkler. Wealth of networks: How Social Productions Transforms Markets and Freedom. 2006

[12]HOFFSTEIN J, PIPHER J, SILVERMAN J H.NTRU : A ring - based public key cryptosystem

[13]LYUBASHEVSHY V, PEIKERT C, REGEV O.On ideal lattice and learning with errors over rings

[14]Bitshares Whitepaper: http://docs.bitshares.eu/_downloads/bitshares-general.pdf