MOLD Whitepaper

The Decentralized Game Platform for The Next Generation

MOLD Team

May 1st 2018

Edition 1.0

摘要

MOLD是一种公平、安全的分布式游戏平台，支持新游戏的开发，简化游戏内的物品、武器及护具等有价值数据的交易，MOLDS通过其MOLDS链上唯一定义的代币，使游戏内的物品、武器及护具等在市场上流通，无需通过第三方机构即可完成交易。与以往的中心化游戏体系不同，MOLD中代币的所有权并不归属游戏运营方，因此赋予了在游戏这种虚拟空间内的数据的全新价值。随着技术的进步和人类的发展，在虚拟空间中产生的这种新价值开始拥有更为现实的价值，蕴含了逐步带来巨大经济效果的可能性。同时，为维护公平，MOLD中的交易可由用户核实且资金流动为可见形式，以抵制伪造货币、重复转让以及其他形式的欺诈行为。以往的货币系统是采用客户端服务器网络模式，其中心化的支付系统容易受到黑客入侵等外部攻击，因此需要花费较高费用来实施复杂的流程并保证运行政策得以实施。在具有P2P网络结构的分布式货币体系中，信息不会停留在一处，不依存赖于第三方，这种机制安全性非常高，并且对系统负担较低。

目录

Glossaries

MOLD : 包括MOLD链在内的所有游戏平台系统
MOLD 链:由分布式社区管理的区块链
mold币：内部流通的游戏代币
社区：MOLD网络所有成员
用户：MOLD网络成员
玩家：MOLD游戏玩家
物品代币：代表某物品所有权的代币
BFT:拜占庭容错
PoI:重要性证明（Proof of Importance）
PoS : 权益证明（Proof of Stake）
PoW :工作量证明（Proof of Work）
验证员：确认交易数据端的人员
参与者：使用MOLD网络的人员
发言人：随机选择的发送交易数据者
视野：生成区块的一个过程

1 简介

1.1 我们的愿景

MOLD致力于打造虚拟空间里的“第二世界”。作为一个平台，MOLD尤其支持新游戏的开发，以及建立一个免费的RMT市场。我们的目标是让人们摆脱体力劳动，创造一个可能通过游戏实现收入的世界。为了实现在虚拟空间世界中创造经济价值这个最终目标，我们将会全力支持完全沉浸式VR游戏的开发。

MOLD是一种公平、安全的分布式游戏平台，可支持新游戏的开发，简化游戏内的物品、武器及护具等有价值数据的交易。游戏内的物品、武器及护具将被视为区域链中的数字财产加以保护，玩家之间可自由地进行交易而无需通过第三方。与以往的中心化游戏体系不同，MOLD中代币的所有权并不归属游戏运营方，因此赋予了在游戏这种虚拟空间内的数据的全新价值。目前消费者对消费者之间的交易已很普遍，因此游戏中多元化经济的出现将会催生游戏内私有财产的产生。

MOLD交易保持公平，可以通过用户验证，资金流动清晰可见，抵制假冒或货币双重转移等传统欺诈行为。在传统的货币体系中，由于它是一种具有客户/服务器类型网络结构的集中式支付系统，因此易受外部攻击如黑客攻击，并且会对于财务调控和繁琐的处理收取很多的手续费。具有P2P类型网络结构的分布式货币系统，由于信息不依赖于一个地方且不依赖于第三方，所以其结构的负担较轻，可以说是非常安全。

1.2 分布化社区的操作原则

建立MOLD分布式游戏平台，操作框架将以社区为基础，成员之间相互合作，并全部支持MOLD准则（见A）。这样一个令人激动的未来目标将通过建立一个没有中心运营商，面向下一代的游戏平台实现，并得到游戏社区内来自世界各地的游戏币持有者，玩家以及开发者在内的利益相关者的支持。本白皮书内容只是MOLD团队做为游戏社区内普通成员的提议，还需通过社区内部讨论进行相应修改。

1.3 定义：mold币

本白皮书中提到的“mold币”依据MOLD链定义。一枚mold代币(ERC20)符合以太坊为基准的ERC20代币，则被称之为mold代币(ERC20)，并可认为其与mold币不同。另外，mold代币(ERC20)与mold币应等值，一枚mold币可交易一枚mold代币(ERC20)。并且，当mold代币(ERC20)与mold币交换时，前者即被销毁。

2 背景

2.1 游戏产业的进化

近年来，随着MOBA（多人在线竞技场）、FPS（第一人称射击游戏）、RPG（角色扮演游戏）、尤其是MMO（大型多人在线游戏）的兴起，PC游戏市场得以显著和持续的增长。此外，由于智能手机与新兴技术革新的普及，移动端与虚拟空间的游戏市场均正得以迅速增长。2014年国际游戏市场规模约为5700亿美元，2015年为6900亿美元（同比增长约25%），2016年则增长至8900亿美元（同比增长约29%） 特别值得一提的是电子竞技市场的增长。这一市场的规模从2015年的3.5亿美元上升到了2016年的4.6亿美元（同比增长30%），且有希望在2019年达到11亿美元。人们工作方式的根本转变看来是此增长的潜在原因。由于科学技术的进步，体力劳动和人工操作将最终被人工智能和机器人取代。因此，大多数人将从劳动密集型行业中被解放出来，并将能够追求更高的生活质量和娱乐。互联网的发展使在线交流更容易实现，从而在游戏空间内形成了多样化的社区。由于AR和VR技术为我们提供了越来越真实的游戏体验，使游戏越来越接近现实生活。

2.2 游戏产业面临的问题

在传统的游戏架构内，游戏内的物品所有权归运营商所有，玩家无法将其视为游戏中的私有财产。在某一游戏中获得的物品的电子信息只能在该游戏中有效，而无法将其价值在不同游戏中之间进行流通。在游戏中投入的大量金钱和时间仅某一游戏空间中持有价值。此外，大多数游戏运营公司有条款明文禁止在游戏中进行物品交易，这使得玩家难以将在某一特定的游戏世界外共享任何电子信息的价值。因此，在游戏世界中玩家的经济活动受到了限制。游戏物品或信息的交易被称为RMT（现实金钱交易），但是许多现有游戏基于中心化的框架，并对上诉的游戏条款和规定中对RMT进行了明文禁止。然而分析认为，市场对于该概念的需求巨大，预估其市场潜力将会在几十亿美元以上。在传统的中心化游戏架构中，游戏发行方需要向集中的第三方运营商支付巨额的发行费用。为了进一步推动发展并创建一个有吸引力的新一代虚拟空间平台，有必要创造一个能转移和交易虚拟物品所具备的电子价值的游戏环境。

MOLD可将游戏内数据转换成代币，使其能在虚拟世界开展分布式的交易，从而形成一个分布式的第二世界。玩家将不再受到中心运营商所设置的规定及其他规制的限制，从而可以将游戏内物品作为自身的数字资产，并拥有购买、出售和获取利益的自由。近来，市面上出现了推进建立RMT交易的动向，而MOLD则意欲将放弃传统的中心化框架，转而打造一个基于区块链技术的分布式的RMT交易系统，关于细节将在以下章节详述。因此，这是一个“属于玩家，来自玩家，为了玩家“的游戏平台，将创造一个面向下一代的分布式虚拟空间世界，帮助所有游戏爱好者都能进行各种经济活动。

2.3 区块链产业趋势

2.3.1 区块链技术的出现

2008年，随着中本聪《比特币：对等电子货币系统》[1] 白皮书的发布，以及比特币的后续发展，比特币被誉为货币及现金的革命性创新。此外，比特币是第一例无需黄金兑换率和中央货币当局背书的数字货币。比特币的基本管理基于区块链技术的应用，通过采用简化的算法以及计算能力，实现了在分布式网络中的台账管理。由以太坊基金监管的开放源以太坊[2]项目是新一代的智能控制和分布式应用平台。以比特币和以太币为主要代表的大多数加密货币的核心均采用区块链技术。（电磁信息的）加密、时间戳、一致性算法和经济激励结构，使分布式管理的P2P交易节点无须类似中心运

营商的授权、计算，避免了高成本、低效率、电子信息存储的安全等问题。虽然区块链本身已不被认为是一项新技术，但P2P通信、加密技术和数据结构在链上的结合，可以被认为是一种创新。

2.3.2 区块链产业面临的问题

分布式管制系统的发展吸引了大量区块链项目，并在全球范围内不断增加，许多应用应运而生。从遵守以太坊智能合约的数字货币应用，到基于纹波协议的全球交易系统，每天都在产生各种不同的应用场景，这些对区块链提出的不止是需求，而更是挑战。

与大多数软件不同的是，分布式区块链结构不要求用户更新客户端和协议，因后者会使得系统由于“硬分叉”或“软分叉”而受到严重限制，从而导致协议更新期间社区协调遭受严重损失。关于区块链可扩展性问题目前仍有争论，因其有可能阻碍比特币协议的发展。由于比特币链的容量有限，如超过百万个交易会引起阻塞，用户面临昂贵的费用来加速此类交易。以太坊也面临类似的问题，即通过使用硬叉作为DAO问题的补救方式，则有可能分裂社区，从而导致用户体验的下降。在当前氛围下，众多炒作项目并不涉及区块链技术，只是为了迎合持续不断的加密货币潮流，一个案例能否做到上述挑战并实现分布式社区目标，将是至关重要的。

3 MOLD 准则

3.1 玩家受益系统

传统上，通过付费购买和在客户端游戏赚取的游戏物品的所有权属于游戏运营公司，而不是玩家本身所有。因此，玩家无法自愿购买或出售游戏内物品，当玩家转向另一个游戏时，这些物品则变得毫无价值。这里必须反复强调的是，在游戏中获得物品的是玩家本身，因此玩家要求得到物品的所有权是完全公正合理的。通过MOLD游戏平台，玩家可以通过在区块链内将游戏内物品代币化（详见第4章），保证电子信息的安全，因此得以建立一个玩家所有的代币物品经济，而不同于以往的游戏公司。通过MOLDEX模式（详见第4章），玩家可以在MOLD平台将代币物品转换为mold币（货币基准利率）。当一位玩家离开A游戏时，他可以将A游戏中获得的物品代币化，并交换成mold币。玩家可以将此mold币用来购买B游戏中的物品。采用这种方式，通过MOLD游戏平台，实质上被（传统游戏公司）禁止的RMT交易则成为可能。通过MOLD，在某游戏中获得的物品价值能够得以保存。在一个不断进化的游戏世界中，通过管理游戏中的数字资产，玩家可以享受到更多自由和更吸引人的下一代分布式的虚拟世界。

3.2 简化游戏开发者工作

许多游戏开发者面临着所需设计与技术的困境，但资金不足以继续开发游戏。此外，主流公司使用的传统中心化平台的商业模式会向开发者收取30%至50%的费用。这种情况下，不仅难以保留开发流行游戏所需的技能，而且也使得开发人员和技术人员难以提高收入。（最好显示数据）然而，在分布式系统中，收取费用不会达到1%。开发者在MOLD分布式游戏平台发布游戏的费用为0.(B)

关于MOLD平台上游戏开发的费用，首先是在平台上的ICO首币发行系统（详见第4章），这使得中小型游戏企业（如传统模式里大公司的分包商）有机会在完成开发之后以低廉的价格在MOLD平台发布原创游戏。除包括游戏物品代币化在内的所有功能之外，还将准备SDK用以支持传统游戏开发人员（详见第4章）。

3.3 下一代游戏的倡议

在当前的游戏行业中，玩家对游戏中的数字资产没有所有权，并且中小型游戏公司和开发者们只作为大公司的分包商。这意味着在此商业模式下主要收入将集中流向大型游戏公司和现有的中心化游戏平台。此外，尽管越来越多的玩家投身于电子竞技领域（职业玩家），公众普遍还是认为沉浸在游戏中是无益的，是逃避现实的手段。这种看法背后的一个原因，是人们认为在游戏中花费时间和金钱所获数字物品的所有权不归玩家所有。如果花在虚拟空间中的时间能影响真实世界，公众看待游戏的观点将会发生巨大的变化。
虚拟空间本身有望变得越来越真实。在这一点上，让我们来比较一下当前和下一代游戏的状况。

下一代游戏将为玩家提供数字资产所有权的官方保证，使他们更加独立，并且随着电子竞技的普及，专业玩家将更为大众所熟知。同时，对于中小型游戏公司的开发者来说，他们将有可能筹集资金，组织项目团队，开发创意游戏，而不依赖于大企业的平淡形象设计。由于科学技术的进步，机器人和AI（人工智能）正逐渐取代人类的劳动和工作负荷，而娱乐在这样一个多元化的未来中变得更加重要。此时，游戏不再将被认为是负面的，相反，它将被视为不仅仅是娱乐，而是作为一种职业存在。分布式游戏平台可能是传统游戏产业所面临问题的新的解决方案。下一代分布式虚拟空间平台将使游戏爱好者真正沉浸其中，游戏开发者将拥有更多自由来创造满足玩家需求的新游戏。MOLD将为世界提供这样一个游戏的未来。

4 专为游戏设计的MOLD区块链

4.1 设计目标：创造一个令人激动的未来

MOLD旨在创建一个基于区块链技术分布式的下一代游戏平台，为所有人提供一个令人激动和振奋的新世界。MOLD将为所有游戏爱好者提供一个系统，让大家都参与创建一个“属于玩家、来自玩家和为了玩家”的游戏平台。

4.1.1 作为数字资产的物品代币

数字资产是一种可编程资产，它以电子信息的形式存在。通过利用区块链技术，数字资产具备高度透明性、保护性和可信赖性，使分销成为可能。用户可以在MOLD链上注册一个帐户并自由管理，将已代币化的游戏物品做为数字资产进行交易。

4.1.2 在虚拟经济中进行安全快速的交易

在MOLD平台刺激自由消费者之间的经济活动，针对游戏将采用定制的区块链，简化传统计费框架，并且在分布式的游戏平台做到对物件代币交易的透明度和安全性。此外，其重要特性之一是可以实现即时付款，因此快速的特性是十分重要的。并且，还将创建一个系统来支持区块链的可扩展性，以应对新游戏所带来的新增用户。

4.1.3 游戏、玩家和开发者

为了让所有游戏爱好者参与到下一代游戏平台中，将开发专用的区块链，该区块链不仅支持现有游戏，并具多功能性能可由玩家和开发人员获取实现不同的功能。通过在区块链通过智能契约实现代币限量发行，对于玩家来说代币化变得更加简单，使得玩家之间的交易更自由。为实现MOLD平台运作，上述特点都将需要，包括一个更好的协议以保证更佳的用户体验。

4.2 以太坊问题以及TPS需求

通过在比特币所使用的区块链中使用图灵完备扩展公式，以太坊实现了下一代智能合约的可能性。在现实中，许多分布式的应用程序正是基于以太坊合约开发。比特币使用UTXO（未用交易输出）代表其货币，而以太币则是将数据储存在数据链交易状态中，“状态”是指被称之为“帐户”的对象。(C)
“帐户”被视为合约帐户，可由单独的合约密码和EOA（外部帐户）密钥共同管理。这二两种帐户数据的利用状态转移函数并被保存在区块链上，并在满足一定条件时执行智能合约。以太坊做为一个创新的抽象的底层基础平台，其构建的协议能够执行各种分布式应用。然而，随着越来越多的用户使用以太坊网络，问题越来越明显。

由于以太坊网络是一个能够实现几乎所有分布式应用的平台，因此各种项目（不仅游戏）同时在平台上进行开发，造成以太坊平台必须承担巨量的交易，到2018年业已增加到最大上限的30000个未识别交易，而这些交易费用相当昂贵。以TPS（每秒交易）为例，以太坊与比特币相比虽胜出约7到8倍，但显然这不足以应付网络预期的增长。并且，由于游戏行业中需要进行即时支付，这样的不足将会导致用户体验方面的显著降低。目前已有部分关于离链技术的改进讨论，但其实施时机和可行性尚不明确。此外还应该注意的是，当处理DAO问题时系统会回滚，并且社区的某些部分会

由于硬分叉而崩溃。因各种项目的交错，使用以太坊平台会会产生诸如此类不同的问题和风险，为实现MOLD创建自由虚拟世界的目标，一个高质量用户体验的创新框架是极其重要的。

4.3 代币模式

4.3.1 MOLD平台主流货币

在MOLD上，用户可以自由将他们拥有的物品代币作为数字资产进行交易。此时，建议mold币可用作主要货币。当用户买卖其物品代币时，可以与mold币的持有者进行交易。使用mold币作为主要货币进行交易时，可在MOLD平台的DEX(分布式交易所)进行。例如，当用户离开A游戏，玩家可以将A游戏中获得的物品代币化并兑换成mold币。接着玩家可使用mold币购买B游戏中的物品。此外，由于智能合约的交易状态，在游戏中物品代币的接收传送中，mold币可被视为“汽油”。同时，通过准备SDK作为使用mold币进行支付当构架，游戏开发者能够轻松利用mold币作为结算帐户，从而在游戏世界中创建一个围绕mold币的自由的经济体。

本白皮书中的“mold币”定义为建立于MOLD链之上。每枚符合以太坊DRC20协议的mold代币被称之为mold币，并且每枚mold币可以单独使用。将发行的mold币（ErC20）总量为25亿枚，其中3亿枚币将被用于研发团队，其余的22亿枚mold币将于2018年1月发行。有关mold币（ERC20）的详细信息，可通过本公司联系地址索取（(0x52E30201f31283dc5F7928b4198896083F604416)）。此外，mold代币（ERC20）与mold币互相兼容，一枚mold币等值一枚mold代币（ERC20）。当mold代币（ERC20）被兑换成mold币时，代币即刻销毁。Mold币可被游戏各利益方使用，以帮助推动MOLD游戏平台的成长和发展。

4.4 MOLD功能块

4.4.1 钱包和帐户

目前，用户的加密交易通常使用专门钱包来处理。但其涉及许多复杂程序，当同时使用游戏平台的现有服务时，用户体验质量降低尤其明显。然而，MOLD平台上的钱包与游戏ID相关联，且玩家之间能简单快速地实现交易。

MOLD钱包能支持MOLD平台上所有类型的代币，它不只是对mold币，还可以为不同游戏中的代币提供安全保护。此外，与传统的钱包服务一样，除了可利用MOLD钱包将mold币和其他物品代币发送到第三方地址外，它还可以访问MOLDEX（详见4.4.3）来实现用户之间的物品代币买卖。

在MOLD平台参加游戏的用户须首先创建一个MOLD钱包。创建钱包时，每个用户将被分配一个MOLD 帐号。通过该MOLD帐号与生成钱包时的密码登录钱包，用户可以同时管理mold币帐户余额与物品代币，此外还可调试已注册游戏帐户。钱包和游戏账户由MOLD帐号关联，一旦登录钱包，则同时也登录了游戏账户，用户可一次轻松切换到游戏界面。通过使用MOLD帐号将游戏帐户与钱包相关联，用户可以免除以往需要分开管理登录游戏帐户和钱包的繁琐（分别登录钱包和游戏帐户，或者仅在需要进行物品代币交易和购买物品时登录钱包帐户），从而提升了用户体验。对现有游戏而言，通过让游戏公司使用SDK（详述4.4.6）将物品代币化，可实现让通过MOLD平台管理的物品出现在现有游戏中。此时，尚未注册MOLD钱包的传统游戏用户可以通过物品交易生成一个新的MOLD钱包。除此以外，通过聊天、交友和群组功能，玩家之间的互动将更为活跃，游戏之间的界限也将趋于模糊。

4.4.2 代币化

在下一代分布化游戏平台里，玩家将把游戏内物品视为数字资产并拥有所有权，可自由参与交易。在这样的环境中，代币化将是代表平台的最大特色。游戏中物品往常由传统运营商负责保管，现在用户可通过区块链技术可以管理、交易买卖，这样一来，便在虚拟空间里创造了一个巨大的经济体，形成第二世界。

有两种类型的代币，即可替换（可替代的）和不可替代（不可替代的）代币。前者，可作为游戏中常见的解决方案，支持以太坊ERC-20协议。游戏物品作为可替换代币可以进行替换，举例来说Molca拥有的一枚代币与Molna拥有的一枚代币的价值相同。然而，多数游戏中的独特物品的价值不同，这让游戏世界变得更令人兴奋。对于具备独特级别、攻击能力和配套技能的游戏物件，这些状态参数将作为元数据存储在游戏中，并可被转换为不可替换代币。应于以太坊上的ERC-721协议代币，即不可替代的代币。在这种情况下，如果Molca拥有的一枚代币想与Molna拥有的一枚代币欲进行交换，就不能被认为是等价交换。不管是哪种情况，对于任何类型的代币，MOLD平台上的用户拥有对数字资产的所有权，可以利用MOLDEX等（详见下一章）进行简化交易。并且，MOLD将有助用户应用SDK系统处理上述提到的2种代币（详见第4.4.6章）。

4.4.3 MOLDEX与MOLD拍卖

目前，大多数加密交易是通过交换所来实现的。交换所管理方设置一中心化处理手法，就其决策过程来说，该种方法被称之为中心化交换。用户通过钱包将资产发送到交易所钱包，用户帐户余额将由交易所数据库进行管理。资产本身存储在交易所内。因此，用户必须信任交易所，他们的数字资产完全交由第三方（交易所）持有。在中心化交换模式中，有大量的案例可能由于交易所自身原因造成资产丢失或是被发生黑客事件，并导致客户信息泄露。由于单点故障，还存在集中访问和DDoS攻击（分布式拒绝服务攻击）的风险。在这样的情况下，安全交易受到威胁不是由于区块链本身，而是因为交换服务器的崩溃。相反，建立于无中心运营商基础，遵循智能合约运行的交易所被称为分布式交易所。用户自己负责管理资产，并且在交易期间用户可通过钱包将他们的代币发送到合约地址，从而实现了无须通过第三方实现交易。然而，与中心化交换模式相比，由于用户数量少，流动性差，目前还不实用。

基于以上考虑，为实现无须第三方参与的物品代币分布式市场，在MOLD平台中，将建立MOLDEX作为玩家可以自由买卖物品代币的环境。在MOLDEX中，mold币为基本货币，各种物品代币都可以在MOLD平台上进行兑换。因此，Bob可以卖掉A游戏中的物品代币，而从B游戏购买物品代币，然后将其作为B游戏的物品使用。物品代币和mold币之间的兑换率将由市场决定，市场定价反应供应和需求。稀缺性将成为衡量一件物品价值高低的标准，随着玩家在虚拟空间中的经济活动增多普遍，通过MOLDEX进行游戏物品代币交易将产生一个新的虚拟经济体。即使是MOLDEX，因为它目前不便流动所以操作不便，人们正在讨论引进建设中的项目启用此机制来自动确定代币的价格和流通性，使得称为Bancor 协议[3]即时付款方式成为可能。

此外，对于仅少量发行的稀有物品代币，DEX的购买和销售将不足够，因此平台将采用一种叫做MOLD拍卖的系统，在限定时间内通过招标拍卖。由于这一系统是基于智能合约的，因此寻求出售物品代币的玩家仅设定截止日期便可以最高出价出售。

4.4.4 玩家第三方托管交易

如希望直接与游戏社区中熟悉的第三方进行交易，可以利用MOLD平台建立第三方托管交易避免欺诈。举一个简单的例子。Alice 和Bob通过聊天功能成为朋友，双方都同意将Alice在A游戏中拥有

的某件游戏物品与Bob在B游戏中拥有的某件物品进行交换。现在虽然Alice愿意向Bob发送物品代币，但如果Bob心存不轨，那么极有可能Alice将物品代币发送给Bob，而Bob却不将自己的代币发送给Alice。那么，Alice就将成为欺诈受害者。MOLD平台上的第三方托管交易能够使用智能合约。当交易双方将自己的物品代币发送到各自的第三方托管交易地址时，智能合约则自动向相应方发送物品代币，这样Alice会接受到B游戏的物品代币，而Bob则接受到A游戏的物品代币。因此，若Bob 未能在限定时间内将自己的B游戏物品代币发送到第三方托管交易地址，Alice则可以通过智能合约内设定的时限防止错误发生，按规则她的地A游戏物品代币将被返回。

4.4.5 MOLD 初始代币发行

当前，许多MMORPG和SMS类游戏的开发都是由中小型公司根据大游戏公司的分包合同来完成的。象移动客户端类似的开发应用甚至能由个人完成。因此以往为了创建新游戏而不得不与大型游戏公司联合的方式已经在不断发生改变。

在MOLD平台，将建立ICO（初始代币发行）系统，旨在为所有人提供可自由招募团队或是吸引投资的系统，包括自由开发人员和资金短缺的中小型企业。提供ICO的游戏开发者可以向社区展示白皮书和游戏设计，向赞助者清楚表达新游戏的想法和优点。然后用户可在社区内部严格审查和讨论之后，再决定是否投资该项目。投资者可以将自己的mold币移交到托管ICOS的游戏开发者提供的合约地址，并收到初始代币。初始代币的持有者将获得ICOS发行方提供的各类优惠，例如在游戏上线时优先获取稀有物品，或是以mold币形式根据智能合约自动获得游戏销售额的X%。从投资者的角度来看，ICO模式不仅仅是支持新游戏，还将允许开发人员募集资金平衡渡过开发周期。这样便能在MOLD上形成一个循环，帮助越来越多的的游戏上线，并且随着游戏的增加，新用户数量也将随之上涨，从而有助于推动MOLD平台的进一步发展。
下面将演示MOLD ICO的简单流程。

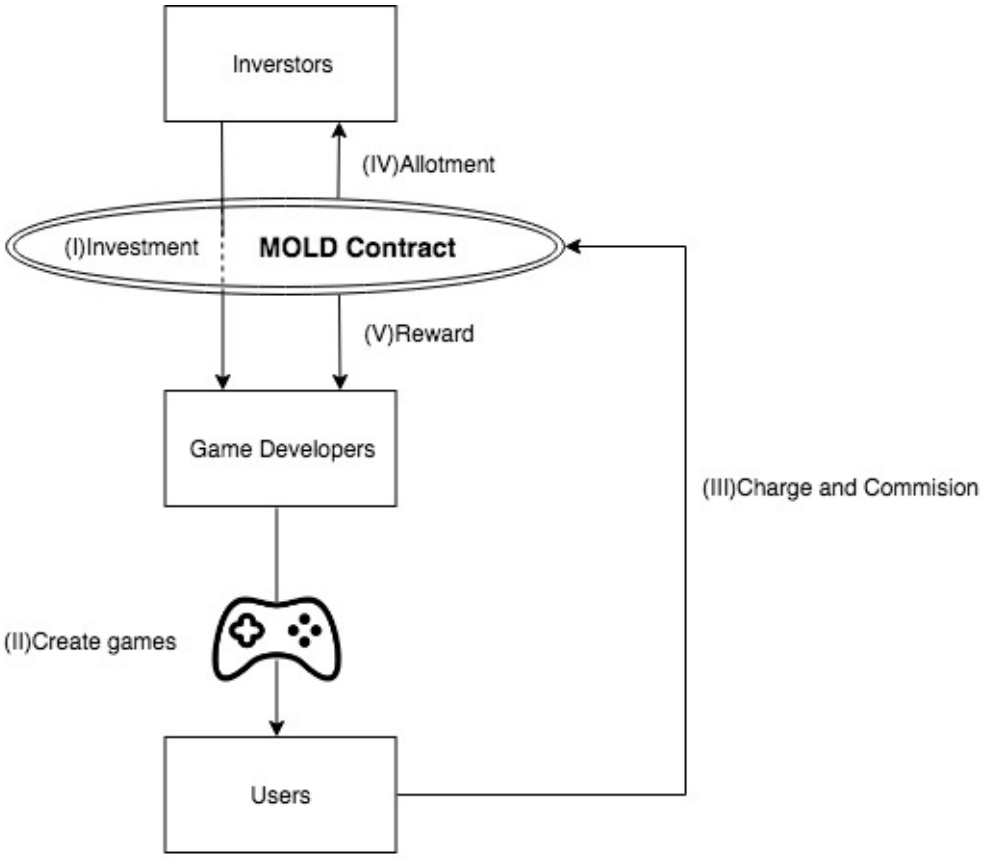


Figure 1: MOLD ICO系统

(I)投资者能够在MOLD平台上以mold币的形式投资某ICO。
(Ⅱ)游戏开发者可以提取由MOLD ICO筹集的mold币作为资金来促进游戏开发。
(Ⅲ)当用户玩游戏时，用户支付或购买物品的费用将被发送到游戏在MOLD智能合约中的地址。
(Ⅳ)根据智能合约，在所产生的销售额中，预定的回报金额将立即返回给投资者。
(V)在扣除投资者（Ⅳ）的红利后，剩余部分资金即为游戏开发者的收入。

传统上，在建立游戏基金时，资金只能在结帐后才能收回规定比例的红利。游戏公司会积极增加开销从而尽可能减少返回给投资者的利润。并且，事实上分红过程通常长达数月，这进一步阻碍了潜在投资者进入游戏行业。使用MOLD ICO系统，游戏开发者能高效吸引资金，组建团队，从而集中精力开发游戏。由于采用的是"无须信任"系统中的智能合约，投资者也能积极投资游戏项目而不需要担心开发方会有任何不良行为。同时，MOLD ICO系统发布的原始代币中的一部分被作为安全代币，一旦有风险，将与国际法律相抵触。出于此原因，游戏开发者必须遵守每个区域的法律。例如，当托管ICO时，将能够与具有传统授权的资助组织者合作。

4.4.6 MOLD SDK

平台将提供一个SDK（软件开发套件），从而使传统或新兴额游戏开发者均能够轻松参与到MOLD社区里，共同创建一个分布式的游戏平台。例如，当今许多游戏都使用诸如Unity和Unreal Engine（虚

幻引擎）之类的软件创建。通过把使用此类软件创建的游戏物品进行代币化，并提供一套能够实现即时支付系统的SDK，将能够让传统游戏设计开发者轻松适应MOLD平台。在现有其它平台上采用支付系统，需收取高达30%到70%的费用。而在MOLD平台上，使用SDK进行交易开发，将不定时提供例如Java之类的各种语言支持，相关SDK将支持每种编程语言，例如对于游戏开发将提供C#类的对口语言。

4.5 区块结构

参考以太坊区块结构[4]、MOLD区块链上的区块由被称之为信息聚合的区块头和交易组成，区块头中包含信息，如下图所示。

- PreviousHash：前一区块头的哈希值
- Txs Root：交易树根节点的哈希值
- StateRoot：状态树根节点的哈希值
- RecepiptsRoot：接收树根节点的哈希值
- TimeStamp：区块形成过程中的适宜UNIX时间
- Height：0创始区块的数量
- Nonce：64位随机数或字符串
- NextMiner：下一个矿的合约地址
- Transactions：交易清单

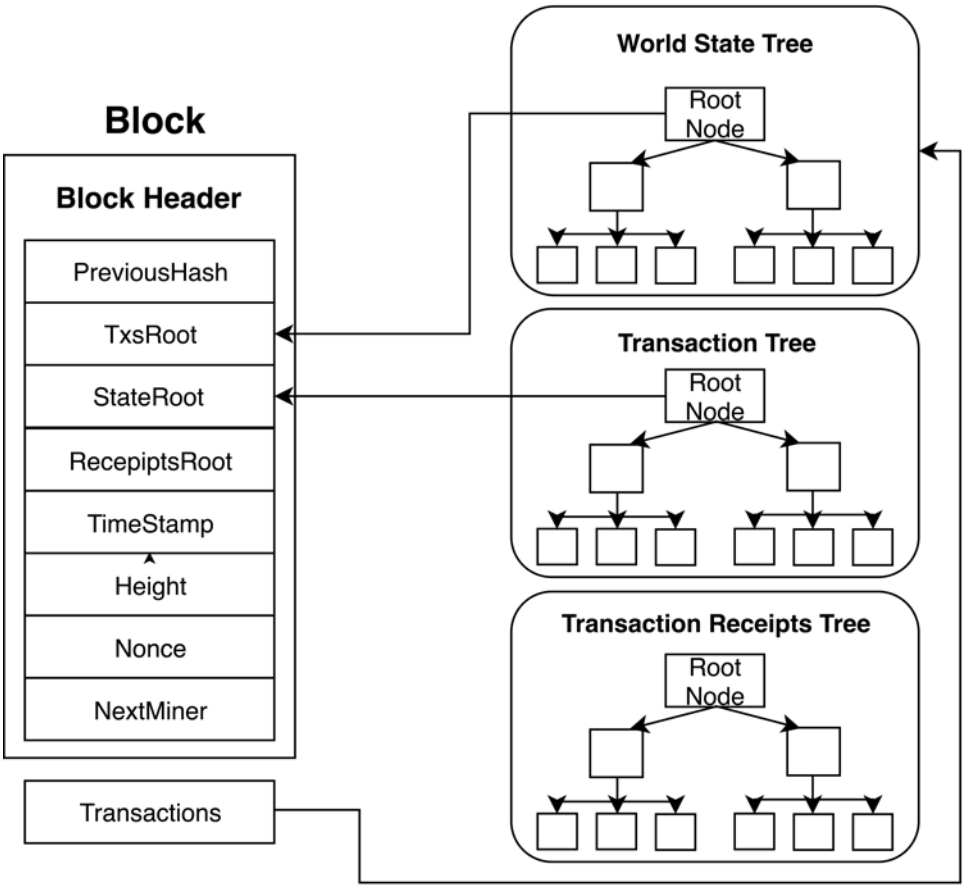


Figure 2: MOLD 区块结构

交易类型有2种，即实际mold币的传输和物品代币的传输。两者在MOLD区块链上区别明显。如果是mold币的传输，将会采取比特币所采用的UTXO方式以及根据每次传送所计算的余额。由于其采用的是UTXO方式，可同时进行并行处理，从而使一个人可以向多人发送。UTXO的每笔交易将会采取类似SHA256函数进行技术加密，且于Merkle树生成TXS根。存储在区块头的部分将成为TXS根的一部分。相反，在生成物品代币期间，代币的合约将会生成并作为帐户状态保存到每个帐户。此外，帐户状态或显示所拥有的物品代币信息的帐号状态，将依据MPT（梅克尔帕特里夏树）来进行散列，由此所有经由哈希编译的帐户信息将被作为状态散列存储在区块里。在合约帐户中，采取以帐户为基础的方式，用以记录在某一点帐户内的物品代币类型。

4.6 共时演算法

4.6.1 共时运算法所面临的问题

目前广泛使用的共时运算尚未能够满足实现本文4.1章中提到设计目标的运算需要。POW共时运算是零和博弈，建立在矿计算能力的执行授权过程上。具体而言，它为完成巨大负荷的哈希运算初始节点提供授权。由于当前不断增加的交易量，需要超级巨型计算机和大型服务器才能解决困难，从而导致消耗大量的电力，并且易遭受攻击率上升51%。此外，由于规模经济，大规模矿将占据优势。规模经济意义上，一个能够将成本提高至1亿日元的矿对比只能将成本提高至100万日元的矿，前者

能够获利100倍。其中部分原因，是由于大规模生产所带来的成本削减效应，以及在网络中占据了有利的地理位置。并且，在PoW中有一个未指定数量的授权过程，不可避免地导致批准过程过于耗时，不适用于要求即时支付的游戏。

PoS 是一种根据拥有代币年限和体积量提供授权的系统，不存在PoW所面临的巨大功耗问题。但也有可能是由于拥有足够资本的投资者拥有生动区块的主动权，从而造成求过于供的情况，降低了货币流通性。而在PoS中，生成区块相对容易，因而能够“无风险”生成区块。

4.6.2 BFT系统（拜占庭容错系统）

PoW和PoS系统面临着不确定性和一些性能问题，BFT[5] 则解决了这些缺点。不同于PoW和PoS，区块是在在验证器决策之后生成的，因此不会在区块链中生成分岐歧。因此，当确认区块未被翻转时，它能够确保其最终性，并且在达到如PoW之类的标准之前，不再需要进行多次计算，从而使得系统性能十分高效。为实现智能经济，NEO采用了dBFT，而Linux基金会则一直在推动Hyperledger Fabric项目（许可制区块链平台）采用PBFT（实用拜占庭容错算法）。假设有验证器成为DBF暂时领导者，持有恶意意图，则其他验证器将监控其行为，并且当确定其欺诈行为时，新的领导者可申请且多数同意后将其替换，这样由此形成容错但不失强大的运算。当发现某验证器有恶意意图（包括具有错误功能的验证器）时，这样的验证器将被排除在验证器池之外，并没收其所存储的任何mold币（参见惩罚性算法）。关于N个节点的一致性系统，拜占庭容错提供了f = (n-1) / 3容错。这保证了系统的功能性和稳定性，节点误差一致性没有超过“ (n-1) / 3 ”的数值。区块链的总分类账由bookkeeper节点维护，并且通过节点通常不参与一致，简化了一致序列过程。这种容错能力确保了安全性和可用性，适用于任何环境。

区块链是一个分布式的分类系统，通过P2P网络连接参与者，在其中广播所有的消息。节点有2种角色：普通角色和簿记员角色。普通节点通过系统传送和交换以接收分类帐数据。而bookkeeper节点为整个网络提供帐目工作来维护分类帐。传递信息的真实性和完整性将通过加密来保证，同时要求发送者将签名附加到发送信息的哈希值中。

在MOLD平台的一致性算法中，将从某节点选择N数量的符合标准的人作为验证员池（参考验证器的选择方法）且所有人都能提供一定数量的mold币，以确认他们作为合适的验证员参与记账。从0到n-1向每个验证员提供虚拟随机数，并在每个周期进行确认。在每一周期的确认工作之后，每个验证员都可自由选择是否继续下一轮验证工作。通过对MOLD的贡献值，从节点池顶部选择验证员进行补充。

4.6.3 验证员的选择方法

MOLD排名是根据钱包中所拥有和使用的mold币数量而定的。MOLD排名参数与钱包mold币拥有量和使用量相关。想要成为验证员的节点先在节点池注册，这里是潜在验证员的初期名单。在注册到节点池中的节点中，最高级别的N个用户将被授予作为验证员的权限。

4.6.4 区块生成过程

区块生成过程

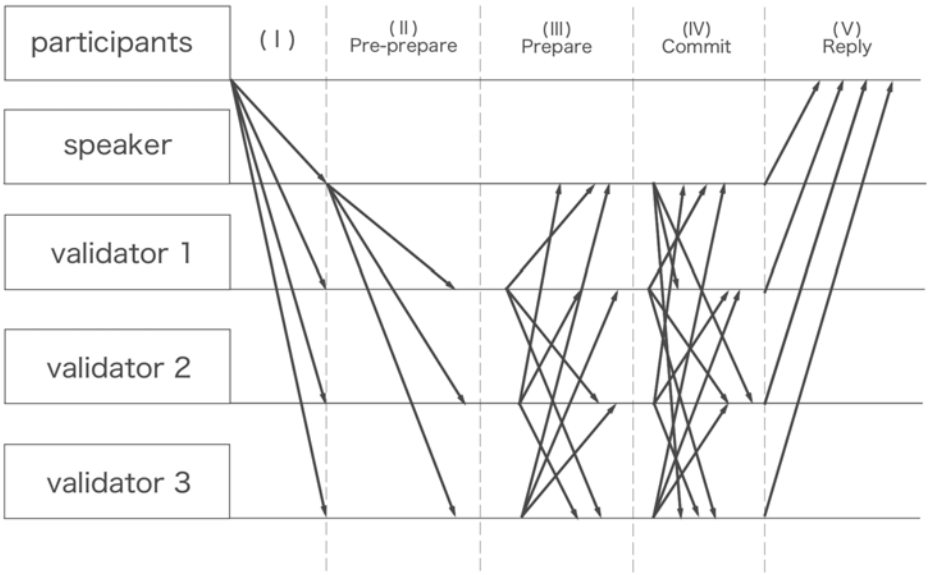


Figure 3: BFT Block Generating Algolism

校验器被分发从0到N-1个虚拟随机函数。

(I)参与者通过网络，发送由发送者签名的交易数据，所有验证员将数据存储在它们的存储器中。

(II) (Ⅱ)从虚拟随机函数中指派的验证员0号将作为发言人发送预准备请求。

(III)验证员发送预准备，以确保其他验证员正确接收交易数据。

(Ⅳ)验证员将检查区块内的数据，并仅在数据有效时发送到所有其他验证员，在验证员内达到n-f一致性，新的区块生成。

(V)最后，通过验证员标示之后，区块被连接到链。

此后发言人的角色将转变为1号虚拟随机函数验证员，重复（i）至（v）的步骤。在周期内，N数量的验证员将有机会至少成为一次发言人，但如发言人不能成功操作，该视图将被改变，并将选择下一个发言人。
如果在验证员中存在非法交易，则验证员将发送一更改视图。如果无法达到n-f一致性，则虚拟随机函数选择的下一个验证员将扮演发言人的角色。
参与者的交易数据包含发送者的签名，使有恶意企图的验证员不可能篡改交易数据。

4.7 惩罚算法与验证员奖励

为使验证员正常运行，需要冻结一定数量的mold币作为存款，一旦对网络有任何恶意行为，验证员会被系统设定失去权限，扣除存款中的固定数额。MOLD网络费用（发送费、部署智能合同、召唤呼叫）被视作为验证员的奖励。通过销毁具有恶意企图验证员的存款，将可提升mold币的稀有性和价值，这也是作为对任何怀恶意企图验证者的惩罚。

5 Molca 工程

Molca项目于2017年11月前后由社区自发启动，它使用一个名为“Molca”的仿人界面作为MOLD分布式平台的向导。除了作为MOLD项目公关活动的媒介之外，Molca已经成为MOLD游戏平台内的标志性角色。未来，作为虚拟YouTube明星的MOLD平台公关代表，Molca计划将可自由地穿梭于MOLD平台，以提供诸如游戏教程和用户支持等帮助。

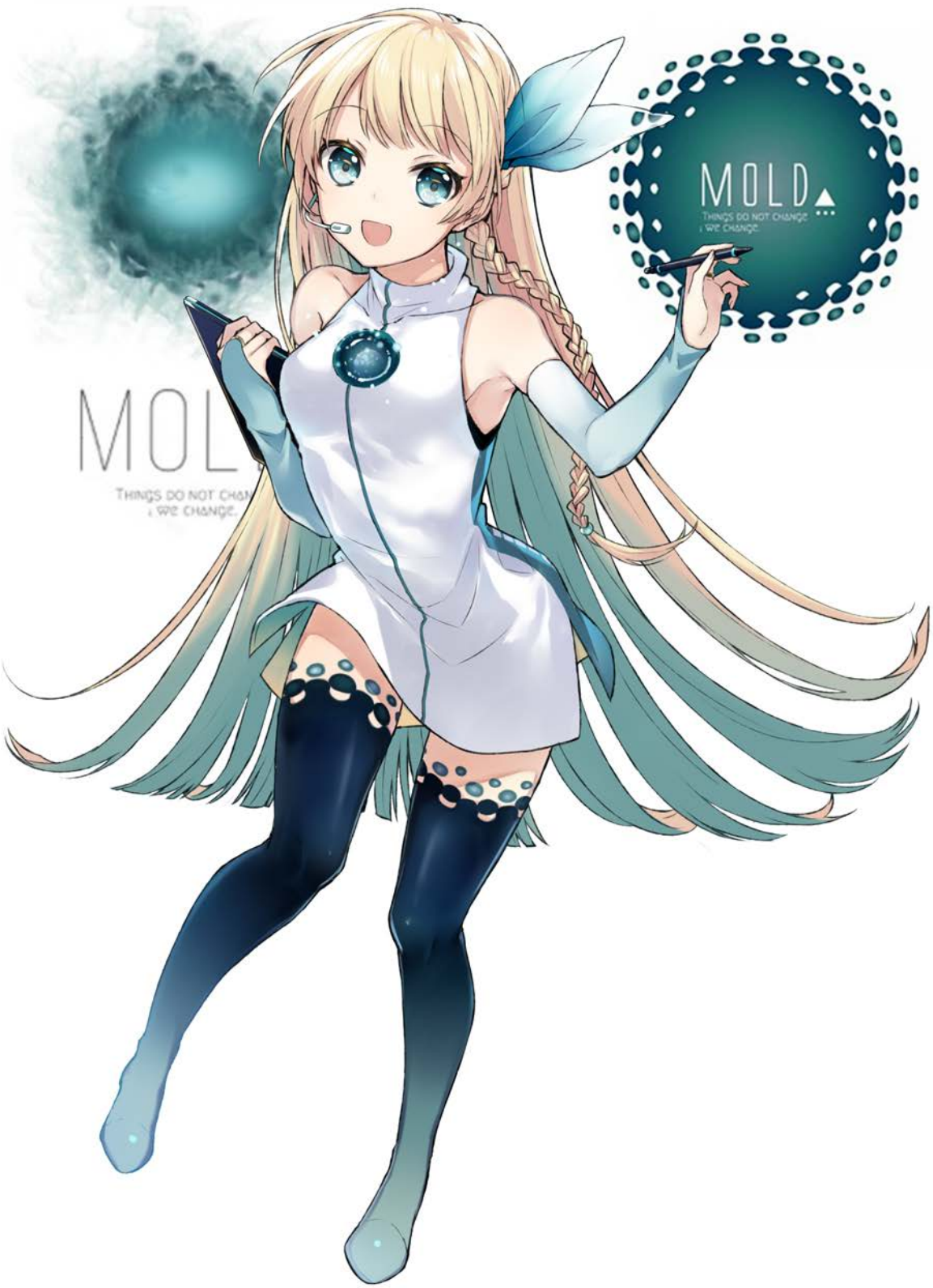


Figure 4: MOLD Official Character “Molca”

6 结论

区块链作为一种无需中心化第三方认证的P2P（点对点）真实交易技术，通过比特币的普及而发展起来，并且因其在抗篡改、高度可用这些革命性的科技而大大节约运营成本，引起了业界的广泛关注。除了货币兑换和支付手段等方面，在国际货币兑换和物联网方面也有诸多贡献，目前已在很多领域进行了实证研究。无论如何，区块链的实践还远未被实现，事实上它们仍然处于发展阶段。2017年，各种区块链项目得以启动，通过ICO筹集资金的活动十分活跃。然而，在某些圈子里，就有很多打着区块链旗号通过ICO进行巨额融资的欺诈案，实际上这些根本无需用到区块链。由于“无须信任”和“无须允许”是区块链的核心价值，任何忽略这些价值的项目实际上与传统系统没有什么不同，在创造下一代平台方面也不具任何革新性。事实上，要理解区块链项目的重点要从根本上理解区块链的关键概念，比如社区支持项目、代币的意义以及产品本身。从本质上讲，社区是开源的，是秉持非盈利信念的自下而上的生态体系，不同于现今从上而下的商业生态体系。代币以所有权表明价值，虽仅仅是电子数据，但在虚拟世界创造新经济的过程中起着重要的激励作用。产品本身就是使用区块链的技术成果。如果社区和代币的存在没有价值，只有一个产品不能足够吸引区块链项目。由于区块链应用情景案例还很少，因此建立应用情景，将有助于实现未来区块链项目的潜力。

由于MOLD平台具备区块链项目的因素，全世界有众多项目希望能够运用区块链技术，为实现在游戏中建立应用情景，有必要创造一个基于实用性和扩展应用性的区块链。为了实现这一点，MOLD将建立由用户掌握物品所有权的方式，从而专注于游戏内物品的代币化，开发MOLDEX以便促进用户之间的简单交易，并且在MOLD平台内为游戏开发人员设计ICO系统和SDK软件。除了基于社区的运营之外，MOLD还将mold币当作主流货币并且赋予代币价值，创建一个能够改变传统游戏，实现虚拟世界代币经济的分布式游戏平台。

另一方面，MOLD还将充当改变人们对游戏既有观念的公众大使，并展现它的改变。任何时候，如果有玩家对游戏感到“厌烦”了，可能是他们看不到游戏的目标和未来。也许人们还认为游戏只是一种娱乐形式，与现实世界没有任何关联。然而，随着电子竞技运动的发展，全世界对于游戏的传统概念都在发生转变。此外，区块链技术虽然其仍处于发展阶段，但其将能够以分散的方式存储数字数据，同时具有防篡改和高可用性。玩游戏对于现实世界毫无裨益的观念，很快即将一去不复返了。今天，我们正处于游戏产业的前沿，游戏将能够给人以荣誉和成就并且震憾撼现实世界。反思整个时代，MOLD作为一个分布式的游戏平台，能够懂得玩家的心思，并且为游戏提供全新的价值。也许每一位玩家对于感觉、荣誉和成就的理解是多样的，但MOLD旨在重新澄清这些模糊的概念，并承诺建立一个“完全自由与现实”的虚拟空间。我们相信年轻一代正是新时代的创造者。

MOLD:为了所有游戏爱好者
MOLD: For all the games enthusiasts

References

[1] Satoshi Nakamoto. “Bitcoin: A Peer-to-peer Electronic Cash System.” https:/bitcoin.org/bitcoin October 2008

[2] Ethereum.https://ethereum.org

[3] Eyal Hertzog. “Bancor Protocol Continuous Liquidity for Cryptographic Tokens through their Smart Contracts” https://about.bancor.network/

[4] DR. GAVIN WOOD. “ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER BYZANTIUM VERSION” https://ethereum.github.io/yellowpaper/paper.pdf, April 2018.

[5] Castro M, Liskov B. “Practical Byzantine fault tolerance” http://pmg.csail.mit.edu/papers/osdi99.pdf ,february 1999.

[6] SECURITIES AND EXCHANGE COMISSION, July 25, 2017 ”Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO” https://www.sec.gov/litigation/investreport/34-81207.pdf

[7] Hyper Ledger http://hub.digitalasset.com/blog/retiring-hyperledger-beta-re-opensourcing-soon-and-other-changes

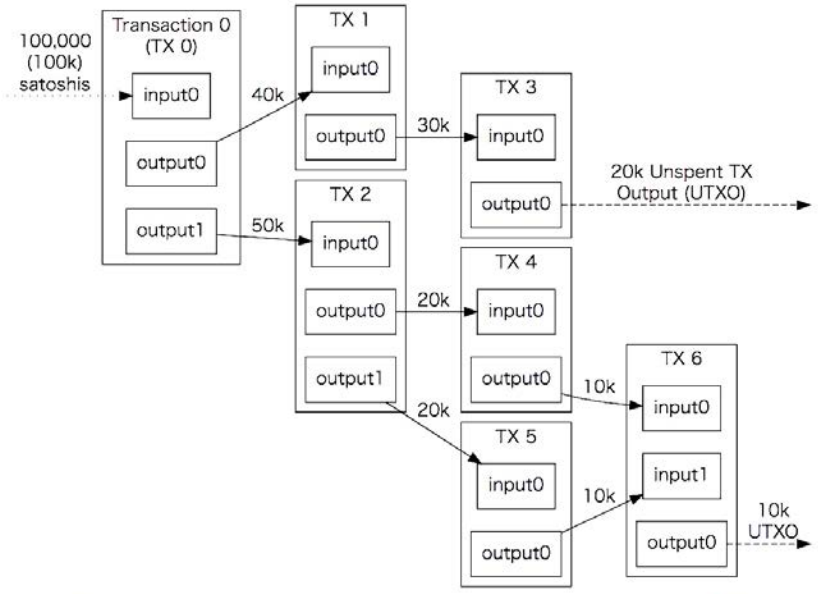
A 分布式自治组织

区块链技术当今备受关注的原因之一，是因为其通过区块链协议除去了中心运营商，实现了分布式自治组织（DAO）。在区块链出现之前，早已有了分布式自治组织的概念。一般来说，由67%或更高比例成员或股东签署合约修改与联合材料的话，这样的组织结构概念上被认为基本相似。但是基于加密理论实现区块链技术的想法却是第一次。随着加密技术市场的蓬勃发展，曾经各种各样的项目都自称为“区域链技术”。然而，区块链技术的本质是倡导一种新的组织管理模式，它是通过改变决策过程和激励结构来实现的。遵循加密理论，MOLD是一个有序持续使用区块链技术的分布式平台，发布游戏的费用为0%，由此促进游戏世界经济活动的进一步发展。基于MOLD链的游戏平台不会采取中心化的运营商，而是分布式社区的操作模式，在这里汇聚了游戏爱好者们对系统的贡献，并且都是无偿的。

B MOLD费用框架

由于MOLD旨在为游戏爱好者打造一个简单和低成本的平台，游戏开发者使用该平台的费用为0%。因此，由于MOLD的运行结构采取的是基于社区合作努力的模式，其中成员均遵守由MOLD制定的原则，因此将没有空间为运营商带来经济效益。MOLD为何不采用收费结构的主要原因，旨在以低成本鼓励更多用户的进入，但关于合法性的讨论也是极其重要的。作为一个应用案例，2016年有一个叫做“The DAO”的收入分配结构被纳入到分布式自治组织之中。关于“The DAO”，2017 年7月25日美国证券交易委员会（SEC）发布了一份文件，指出“The DAO”属于“证券”，并将受到美国证券监管条例[6]的约束。由于收入分配结构可能受到政府的安全条例约束，所以应该考虑到对平台运行造成的可能损害。

C UTXO 与帐户



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

比特币和其它许多衍生币都属于加密货币，是基于UTXOs（未用交易输出）模式来管理的。通过从以往交易历史收集UTXOs，然后创建其他新的UTXOs，这样的UTXOs将被作为未来交易长久的货币形式。此时，每个UTXO在概念上都可被看作是与现有的壁垒相类似。由于此方法在比特币之后被众多项目支持，后续被称之为采取UTXOs的超级帐本。[7]

"We are also switching from our simplistic notion of accounts and balances to adopt to de facto standard of the Bitcoin UTXO model, lightly modified. While Hyperledger does not use Bitcoin in any way, the Bitcoin system is still extremely large and innovative, with hundreds of millions of dollars invested. By adopting the Bitcoin transaction model as standard, users of Hyperledger will benefit from innovation in Bitcoin and vice versa, as well as making Hyperledger more interoperable."

关于区块链网络的一致性系统，关键在于参与的所有节点都将按相等的顺序处理交易，以得出可比较的结论。因此，为了获得参与者的共识，将需要执行并行过程和规模扩展，此时发生交易的基本体系至关重要。与比特币采用的UTXOs模式相反，以太坊采用了账户状态转移模式，因此很有必要了解这些模式的优缺点。与UTXOS模式不同的是，账户模式在概念上更接近于管理银行账户，只需保存每个用户余额的状态转换并将其表现为货币。但其也有一些缺点，比如系统可能泄露账户余额信息。关于UTXOs和账户模式的进一步讨论详见下文。

C.1 模式的优点

并行处理

由于没有帐户概念，发件人可以准备多个独立交易并在每个交易中使用完全不同的UTXO，以便可以按任何顺序同时处理可执行交易。一次性可以处理大量的交易成为了这种功能的主要优势。

高度的隐私水准

虽然依赖于所有者如何管理他们的货币，用户可以通过每个UTXOS使用新的钱包，这样一来则难以将账户和地址关联起来。这是货币的一种适宜特征。在帐户模式中，使用这种方法进行隐私管理比较困难，因此需要有一个类似零知识证明的系统。

潜在可扩展性

就某些方面而言，UTXOS模式适用于解决某些可扩展性问题。例如，在一个UTXOS模式中，如果Merkle树的一部分数据丢失，只有货币所有者将遭受损失。在账户模式中，除了所有者之外，所有关联账户也会遭受损失。

可重入到可重入性

由于UTXO仅由布尔函数管理，它不会面临由于意外重入而崩溃的问题。在以太坊初期阶段，DAO攻击是一个大问题。

C.2 帐户模式的优点

简易

在一个UTXOs模式中，当使用钱包管理多个UTXOs时，它需要考虑占用所有UTXOs。但是在帐户模式中，只需要简单地从数据库中读取余额。

可替代性

由于每一组币在密码层都不保存区块链，所以每个硬币都可替换，并且不存储特定信息。

易于参考的轻客户端

虽然从另一个方面来看，轻客户端可以通过遵循帐户模式中的状态树来获得与单个帐户有关的所有信息，但是从UTXO的角度而言，每笔交易都不同于每个参考点，从而使之成为一个复杂的系统。此外，譬如钱包之类的集成服务也变得相对容易。当上述数据结构执行智能合约时，工作负荷将会加大。

注释

此处所包含的信息只用于激发社区内讨论，并非为了促进MOLD的销售或相关公司的股份或证券。任何此类恳求都将按相关法律条款进行。本文所提供的信息和分析不应作为投资判断的依据，也不应包括具体的建议。因此，本文不提供与投资有关或促进投资行为的意见或建议。本文的目的不是为了进行市场营销或推销证券。MOLD不对文中的错误、遗漏或误差引起的任何形式的损失或损坏承担任何责任。此外，文中所刊登的信息如有变更，恕不另行通知。请注意本文件（第1版）今后可能发生改订，并且任何改订都将详细披露列举说明。请参考MOLD网页（https://moldproject.org）确认更新文档版本。

1.因凭证信息丢失而导致的mold币存取风险

购买者的mold币与之前分配的以太坊钱包地址相关联。以太坊钱包的地址由购买方自行管理。如果信息丢失，登录权限的丢失可能导致mold币的损失。购买方必须将私钥信息保存于多个安全场所，或者备份于物理上独立的场所。

2.与买方资质相关的风险

具有账户信息的用户或任何可访问密钥的第三方机构均能够执行mold币相关操作。为减轻这一风险，用户应使用电子设备来防止未经授权的访问。

3.监管措施及法律修订方面的风险。

区块链技术是世界各地监管机构重点审查的主题。MOLD和mold币也可能受到任何调查、监管措施或法律修改的影响，这些有可能对MOLD产生阻碍或限制。

4.因对游戏或分布式应用关注不足带来的风险

可能对MOLD和mold币的关注者仅限于那些关心生产和开发分布式应用，以及对游戏感兴趣的人群，而不包括大多数商业、个人和其他与游戏无关的组织。关注人群有限，可能会对MOLD的发展和mold币的潜在价值产生影响。

5.MOLD低于买家期待值带来的风险

MOLD目前尚在计划阶段，在上线之前仍有可能对内容进行修改。由于设计阶段规划与执行的变更，以及包括MOLD的运行等其他原因，届时购买者实际购买到的mold币或MOLD的形式或特征可能低于他们的期待值。

6. 因窃取、黑客攻击等造成的风险

黑客以及其他团体或组织可能会通过拒绝服务、Sybil攻击、欺骗、拆分洗钱、恶意软件及基于协议的攻击等各种手段，对MOLD或mold币的使用性带来破坏。

7.因加密技术中的脆弱性及易损性带来的风险

随着加密技术和量子计算机的进步，在加密和MOLD领域可能会出现更多的风险，导致mold币被盗或丢失。

8. 因MOLD的使用或用途不足带来的风险

虽然mold币不应被视为是一种投资，但其有可能将具有长期的价值。如果MOLD未得以充分利用或使用，mold币的价值可能是有限的。如果上述情况成为现实，则该平台在起动阶段可能几乎没有市场，从而可能会限制mold币的价值。

9. 无保险损失的风险

与银行账户或其他相关金融帐户不同，MOLD平台所拥有的资金无任何保险。当发生价值损失或遗失时，任何诸如联邦储蓄保险公司的公共保险公司或私人保险公司都不会提供任何救济措施。

10. MOLD项目的解散所带来的风险

如果MOLD项目无法得以实施，项目组可能面临解散。无法实施出于但不仅限于以下原因：比特币、以太币和/或mold币价值的不利变化，或缺乏商业关系。

11. MOLD故障所带来的风险

MOLD由系统问题，可能会导致Moldcoin的价值下降。

12. 不可预见的风险

加密代币是一项无法保证的全新技术。除了上述描述风险以外，MOLD开发团队还将面临其他无法预见的风险。上述风险的意外组合或变化均可能引起意外风险的产生。