上海喵爪网络科技有限公司

喵爪币白皮书

建立基于信任的点对点的去中心化学习社区

（第一版）

2016年8月

区块链是什么？

现在看区块链相当于1993年采访互联网一样。

区块链之于现在的世界，真的会像互联网那样对未来世界发挥更重要的作用吗？
凡是推行过价格垄断的经济领域，垄断实验都无一例外地失败了。虽然经济学家反对政府垄断商品价格，但在货币体系这个经济圈，目前央行却依然占据着主导地位。可以预见，货币体系的中央计划未来也难逃式微命运。央行在多年来实行零利率政策刺激经济发展未果后，甚至变本加厉，试图推行负利率措施（一些银行已经开始执行负利率政策），这无疑是将人们带到了一个新的困境当中。

经济学家F.A.哈耶克认为，市场扭曲和商业盛衰周期的原因在于央行对货币和利率的掌控。1974年，他凭借这条理论成为诺贝尔经济学奖得主，此后，他又在70年代发表了一系列文章，认为从长远看，只有给予公司发行私有货币的自由，才能真正地解决这个问题。政府会贬低货币的价值，银行会进行疯狂的信贷扩张，但如果人们能够选择使用何种，他们在交易时就不太可能会使用有风险的央行发行货币。

哈耶克后40年的今天，比特币背后的技术支持——区块链终于获得了它应有的关注。有了区块链这一分布式账本，政府官员和央行职员就无法再干预人们的交易和转账过程。虽然目前比特币网络还处在萌芽期，但未来它的发展会产生革命性的巨大影响，从根本上动摇中央银行的地位。

然而，央行并不甘示弱。目前，央行已经在考虑发行基于区块链的数字货币以取代现金。一旦发行成功，像负利率这类激进的货币政策在区块链技术面前就会无处遁形。

上个世纪时，经济领域的根本矛盾在于在中央计划经济与自由企业的对立。而如今，区块链又开启了新的篇章。区块链导致了多种私有货币的产生和相互竞争，一方面，人们在全球范围内进行交易时有了多种货币选择；而另一方面，央行和政府也可以对发行货币进行完全掌控。

哈耶克的获奖理论还说，央行最终会松开对利率的控制。 随着人工廉价信用(artificially cheap credit) 在经济体制的渗透，央行的刺激手段会失去作用。经济在到达一个紧缩点(crunch point)——也就是Katastrofenhausse后，信用市场会爆炸，而整个经济也将崩溃。

现在，全球的债务泡沫已经超过了200万亿美元（$200 trillion），快速叫停货币体系的中央计划已经是刻不容缓。我们应当将货币体系建立在自由制度和自由企业上，而不是建立在注定失败的中央计划或是价格垄断政策上——区块链正是达成这一目的的武器。

基于区块链的技术特征，喵爪提出众筹重构教育的概念。为什么会提出这个概念，具体怎么重构教育呢？

区块链的概念首次在论文《比特币：一种点对点的电子现金系统（Bitcoin: A Peer-to-Peer Electronic Cash System）》中提出，作者为自称中本聪（Satoshi Nakamoto）的个人（或团体）。

简单来说，区块链（Blockchain）是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。该技术方案主要让参与系统中的任意多个节点，通过一串使用密码学方法相关联产生的数据块（block），每个数据块中包含了一定时间内的系统全部信息交流数据，并且生成数据指纹用于验证其信息的有效性和链接（chain）下一个数据库块。
如果一个系统不具备这些特征，将不能视其为基于区块链技术的应用：去中心化（Decentralized）、去信任（Trustless）、集体维护（Collectively maintain）、可靠数据库（Reliable Database）。并且由四个特征会引申出另外2个特征：开源（Open Source）、匿名性（Anonymity）。

目前现有的主流数据库技术架构都是私密且中心化的，在这个架构上永远无法解决价值转移和互信问题。所以区块链技术有可能将成为下一／代数据库架构。通过去中心化技术，将能够在大数据的基础上完成数学（算法）背书、全球互信等。 根据区块链的相关技术特征，作为区块链未来应用最为典型的领域有：

电子货币
智能合约 证券交易
电子商务
物联网
社交通讯
文件存储
存在性证明
身份验证
股权众筹

喵爪币是什么

我们决定发行喵爪币，用于喵爪星球教育社区及极客豆学院的运营。喵爪币的总量为 3 亿个。分发机制如下：

1 认证批准 20 个喵爪币兑换商：喵爪币兑换商可以独享的优惠条件是以一分钱一个的价格购买 10 万个喵爪币。个人购买及兑换喵爪币将通过喵爪币兑换商来进行。

2. 第一批将对外将发售 3 千万个喵爪币，定价在 0.1 元人民币／个； 或 10 个小贝壳币兑换 1 个喵爪币

3. 用一亿个喵爪币建立喵爪基金会，用于促进喵爪及相关产业发展，奖励相关有贡献的人

4．用一亿个喵爪币用于给出色的 Playlist 投票。

5　剩余部分用于西游 Go 及 MZ 星球教育沙盒游戏运营

喵爪币技术说明

共识机制

喵爪币是公开广播频道的加密原语，并引入一种新的共识算法，Obelisk以及基于Obelisk的Skycoin fork而来。Obelisk并不是一种单一算法，而是一整套采用多种技术来实现特定安全。它的出世是由于比特币给我们的灵感。

比特币的概述-一种拜占庭将军问题的解决方案。

新的交易被放入区块，然后附加到区块链上。比特币网络的任意节点都能创建区块。每个块因此有一个单一的父节点，但是一个或多个合法的后继（子区块）。多个链形成一棵树，并且比特币解决的核心问题是让网络中的每个节点认同到底区块树的哪个潜在链成为共识的区块链。

比特币使用一种称之为工作量证明的技术来决定唯一的区块链。一个合法的区块要求一个低于特定值的哈希值。节点们添加交易到新的区块并且随机的尝试notch直到发现一个具有正确哈希值的区块。

一个函数被用来创建区块树中链的总体排序。拥有最高难度并且要求最多哈希运算才能创建的链称为“最长链”和共识链。采用一种包含“区块深度”和“难度”的标识来创建一个对区块树中所有线性链的总体排序，并且我们接受消耗资源最密集的链作为共识链。

比特币节点们互相之间随机连接，并且每个节点传递它所知道的难度最大的块链到其它节点。如果一个节点拥有一个比其它节点所知道的产生难度更大的链，其它节点接下来将会接受该链。节点将对函数进行求值，来验证接收到的块链的难度更大，并且随后切换到接收到的该链。节点会随后广播它的新链到其他节点。通过这种方式，通过网络来传播共识，并且所有节点达到同一个共识。

比特币并不假定节点拥有标识，并且不假定节点是诚实的。节点能够发送任何数据到其它节点，并且它不能影响共识结果，因为难度是一种能够自己单独验证的设计机制。

比特币的创新

比特币已经完成多种需要我们继承的创新：
- 一种每个人都有一份拷贝的单一数据结构
- 存储金融交易在区块链中（公开的交易总帐）
- 使用PoW和重置难度来实现恒定的区块产生速度
- 使用公钥哈希作为地址（公钥直到使用时才会披露）
- 使用“输出”表示余额。放弃创建可划分的数字现金的尝试：为了从$25的输出中支付$20，发送$20到其它人，同时$5到自己。
- 第一次使用函数（PoW难度函数和区块深度）来定义区块树的总体排序
- 公开的记账规避了传统数字现金双花问题

比特币系统中的缺陷

比特币系统有如下局限性：

- 比特币中的共识结果并不是最终的，并且能被撤回。一个能够租赁或者买到足够哈希计算能力的人或者组织能够撤销交易。
- 比特币获得了网络共识，但是通过控制通过路由的数据包，每个比特币节点非常容易受到控制。一个控制路由器的攻击者有绝对的控制力并且能够任意影响节点的共识结果：攻击一个银行使用的比特币节点比通过攻击整个网络来实现一次双花攻击更加容易。
- 比特币网络的安全基于，对于一个想要攻击网络的个人或者组织，获得绝大多数哈希速率的成本太过于昂贵。这并不是一个正确的假定。随着比特币获得成功和价值增长，攻击网络的动机会越来越强。
- 成功攻击能够从交易平台偷取巨量的数额(最近MtGox攻击事件中价值$400 million)。一个有经验的攻击者能够从交易平台以比特币购买alt coins，并且51%攻击来撤销比特币充值交易。用户因此同时获得了比特币和alt coins，并且交易平台将因为不能兑现破产。
- 攻击者能够从银行和赌博网站偷取大量数额。一个攻击者存储比特币然后提取出来。攻击者通过51%攻击来撤销存储交易，同时保留提取交易。这种类型的攻击会很突然，并且非常有利可图，从而影响比特币的整个服务，这种可能性并不能被排除。
- 随着比特币的成熟，买空比特币或者攻击网络的犯罪行为能够获利很多。在将来，对比特币的成功攻击能够导致数以百万美元计的买空收益。
- 获得绝大多数哈希算力的成本可能并没有高到足够防止特定攻击者。KNC miner已经一万美元单价发售了200个批次，加起来可以获得绝大多数算力。攻击比特币网络的成本低于两百万美金。
- 攻击比特币网络的成本在某些为了抹黑比特币安全性的国家或者公司的资源能力范围之内。对资本控制性强的国家和竞争公司能直接攻击比特币网络来网络他们的经济利益。
- “云挖矿”和第三方算力租赁服务正变的越来越成功。很多大的矿池现在拥有租用算力完成绝大多数攻击的能力。
- 黑客们可以使用路由器和网络设备中的各种安全漏洞来从银行和交易平台窃取比特币。一个攻击者能够控制一个比特币节点连接到的节点，并且确保它连接到黑客控制的节点。一个攻击者可能引入一个存储交易到银行的所在侧链，并且让银行发送一个提取交易到主交易网络。
- 比特币不能低成本的提供安全性。运行比特币网络的成本非常高昂。比特币网络正在使用非常大并且指数增加的电能，并且对环境不负责任。比特币的安全性故意的建立在制造尽可能多的电能浪费之上。一个安全的系统应该让攻击花费多于防守。在比特币中，这个比例是1：1。

- 比特币交易需要平均10分钟时间来打包进入一个区块，并且为了更高的安全性需要的时间更多。比特币基本上不能降低交易时间的同时又不降低安全性。这一点从推广角度上妨碍了比特币的接受度。

这些问题必须被解决。通过这些问题，比特币应该被视为加密货币的胚胎而不是最终形式。未来的货币将显著的改善比特币并且在很多方面超过它。

比特币能够被改善的几点是：
1. 安全性
2. 效率
3. 速度
4. 透明度

1. 一旦一个交易被执行，它应该是不可能被撤销共识的。共识应该尽可能的不可逆。（没有双花，安全性）
2. 运行一个完美的安全的账本的成本应该是极低的。（效率）
3. 系统应该允许交易在几秒级被确认 （速度）
4. 应该很容易审计和识别恶意节点 （透明度）
5. 节点应该能够检测他们的共识是否不同于网络 （路由攻击，安全性）
6. 一些安全属性应该保证完好，即使网络中的绝大多数节点是恶意和勾结的。
我们引入一个称之为Obelisk的系统来达成这些目标。

现实世界中的拜占庭将军问题

拜占庭将军问题是一个学术界用来设计算法来保证计算机网络达成共识的模型。一个成功的共识算法要求所有的诚实节点达到同一个共识。

在拜占庭将军问题中，你有N个将军围困一个城市。将军们仅仅能通过通信渠道来通信，并且所有人必须达到同一个决定。他们必须在同一天同时攻击。为了征服这个城市，所有的将军必须同时进攻或者等待。如果一个将军进攻，所有将军应该进攻，并且如果一个等待，所有将军应该等待。如果一个将军进攻并且其他将军们按兵不动，围攻就会失败。将军们仅仅能通过信件通信，并且有可能不到达或者晚到达。

在拜占庭将军问题的学术版本中，失败是良性的。可能一个将军没有得到信。表述失败但是良性的计算机服务器应该同时到达相同的状态。真实世界的拜占庭将军问题被称之为“对抗拜占庭将军问题”。 对抗拜占庭将军问题发生在当有人能通过攻击网络来获利情况下。

存在一些不诚实的将军，并且他们将不惜一切代价来确保不能达成共识。不诚实的将军们可能撒谎。他们可能告诉一个将军一件事情，对另外一个将军则是不同的事情。不诚实的将军可能杀死另外一个将军的信使，让一个发送的消息不能被接收到。不诚实的将军们可能假冒其他将军的信息。不诚实的将军们能够改变一个诚实将军的信息。不诚实的将军们会互相勾结。

在比特币中，他们甚至走的更远，进行贿赂和破解。他们将猎取你的雇员并且黑进承包商的电脑来获取你的服务器权限。他们将改变系统时钟，攻击路由，使用哈希碰撞，使用数以千计的僵尸网络来拥堵网络并且破解签名延展性。
一个安全的系统必须不仅保护每个已知的攻击，还要足够鲁棒性来进化并且在未来攻击中存活下来。比特币中的一些问题可以被修正，比如签名延展性。其他问题则是基础性的，并且不能被解决，除非定义一个全新的框架，比如对于工作量证明和矿工的依赖性。

喵爪币的安全哲学:

安全性是一种针对威胁进行连续识别和加强的过程。一个良好的系统获得“深度防卫”，拥有多个冗余系统，并且能够在任何单一测度下的完全失效中存活下来。

良好的安全性不仅来自保护来自每个可能的不可预测的威胁的悖论，并且依赖于了解哪些威胁是切实存在的，哪些是仅仅是干扰性的。

良好安全性具有乘数效应。需要花费攻击者10美元才能窃取的一美元才是安全的一美元。

没有一个单一的系统能够获得比特币后继者需要的所有目标。喵爪币采用一个模块化层级的方式，并且使用不同的系统来加强特定的要求。喵爪币被设计为一个具有多层交迭防御的要塞。

喵爪币安全性重点在于保护所有比特币已知的威胁，并且之后每天使用该系统的用户遇到的威胁。喵爪币安全性试图对于可能造成用户，股份持有者和机构，最大损失的攻击类别给予最高界别的保护。这要求对于比特币的完全重新设计，包括钱包生成到区块共识。它

需要具有一定视野，这也是我们一直在努力获得的，并且要求在很多领域实现基础性的创新。

比特币中的大多数损失来自于设计中的疏忽，缺乏可用性，以及发生在终端用户而不是对于软件或者数学的基础性技术攻击。一个用户备份了它的钱包，进行了一些交易，并且重新格式化了他的电脑。他认为他的币是安全的，因为他有一个钱包备份 （不同于他因忘记备份而丢失数以千计美金的愚蠢朋友）。 他加载了钱包，同时他一半的币丢失了。比特币对每一个交易生成新的地址并且作为找零发送币到这些地址，但是新的地址并不在钱包备份中，因为在进行备份时他们还并没有被生成。

喵爪币必须同时解决若隐若现的现有的数学威胁，同时解决对日常用户来说，比特币不完善和考虑不周的用户体验造成的安全风险。比较差的可用性和设计迫使用户对安全性妥协，并且甚至让拥有百万美元的重要用户依赖于不安全的在线钱包。尽管每天媒体都有报道频繁和大额的丢失，到今天为止，更多的比特币由于可用性问题丢失，而非偷窃比特币的犯罪行为导致。

全部现存比特币中超过半数的在它们的初始地址上从未移动过，并且将永远不会。他们仅仅是简单的被丢失了。不可恢复的钱包文件，丢失的钱包，对于文件中真正备份的是什么的误解。MtGox近期报告说在一个他们不知道有比特币的钱包中“发现”了二十万比特币。钱包被忽略，并且因为软件由于钱包“太老”而不能加载钱包文件，认为里面没币而被很轻易的删除 （在很多人身上发生过） 。

大多数的安全问题是在于那个层级上。他们是关于可用性，终端用户以及交易安全性。本文余下的部分包含了一些我们创造的新技术来解决网络层级的安全性，并且保护喵爪币的区块链。

```
func newBlock(prev Block, currentTime uint64, unspent UnspentPool,
    txns Transactions, calc FeeCalculator) Block {
    if len(txns) == 0 {
        log.Panic("Refusing to create block with no transactions")
    }
    fee, err := txns.Fees(calc)
    if err != nil {
        // This should have been caught earlier
        log.Panicf("Invalid transaction fees: %v", err)
    }
    body := BlockBody{txns}
    return Block{
        Head: newBlockHeader(prev.Head, unspent, currentTime, fee, body),
        Body: body,
    }
}

func (self *Block) HashHeader() cipher.SHA256 {
    return self.Head.Hash()
}

func (self *Block) HashBody() cipher.SHA256 {
    return self.Body.Hash()
}

// Returns the size of the Block's Transactions, in bytes
func (self *Block) Size() int {
    return self.Body.Size()
}

func (self *Block) String() string {
    return self.Head.String()
}

// Looks up a Transaction by its Head.Hash.
// Returns the Transaction and whether it was found or not
// TODO -- build a private index on the block, or a global blockchain one
// mapping txns to their block + tx index
// TODO: Deprecate? Utility Function
```

我们已经数学意义上证明我们的系统可以获得共识，拥有我们想要的安全性，并且在正常网络状态下工作正常。我们现有的一些数据结构从未在任何虚拟币或者软件中被见到过。现在我们正在进行可供部署的原型系统开发。喵爪币开发流程是迭代性的。随着我们处理一些细节，解决已知问题，测试系统并获得反馈，将会有一些改动，改进以及重新调整。

公开广播频道：个人区块链

在对抗拜占庭将军问题中，有如下通信假设
- 消息可能乱序到达
- 消息可能不到达
- 不诚实将军们可能对于不同人说不同的事情
- 不诚实将军们可能撒谎
- 不诚实将军们可能伪造其它将军的签名
- 不诚实将军们可能拦截并修改来自其他将军的消息

我们引入一种称之为公开广播频道的新的加密原语并且描述了它的实现。这个原语具有如下属性：
- 你不能对A说一件事情，对B说另外一件事情
- 通信是公开的
- 通信不能来自除你之外的其他人（认证过的）
- 一旦发布，不能轻易的取消发布
- 你不能回溯一次通信而不被检测到 （链接的时间戳/哈希链）
- 消息顺序到达
- 消息在传输中不能被修改

公开广播频道被实现成一个区块链。每一个人可以读取链，但是仅仅拥有者可以对它挖块。为了成为合法的个人链，每个区块必须用拥有者的私钥进行签名。

每个Obelisk节点具有一个个人区块链，并且它是Obelisk系统的核心部分。

公开广播频道强加了几个约束：
- 一旦发布一个区块，它不能被取消发布 （区块被点对点的复制到所有订阅者。一旦一个区块已经被发布，它将扩散到所有订阅者。你必须销毁所有已经接收到区块的节点来从网络上擦除它）。

- 一个节点不能发布一个之前区块的不同版本而不被检测到 （区块被编号并且如果节点使用同一个序列号签名了两个不同的区块将被检测到）
- 在不延迟区块发布情况下，一个节点对于接收到的区块不能回溯时间戳 （时间戳仅仅增长，时间戳随着区块序列号单调增加）
- 链中的一个区块不能在不报废之后区块情况下被修改 （哈希链，每个区块头部包含之前区块的哈希）

Obelisk:

每个Obelisk节点（喵爪币的共识节点）拥有一个公钥（一个标识）和一个个人区块链（一个公开广播频道）。共识决定和通信发生在每个Obelisk节点的个人区块链内。这是一个该节点所有事情的公开记录。这让社区可以审计节点是否欺诈和勾结。它给予了社区一种方法识别正在参与网络上攻击的节点并且公开了网络如何进行决定，并且哪些节点正在影响那些决定。

每个节点具有一个它所订阅节点的列表。具有更多订阅者的节点可以更加被信任并且在网络中产生更大影响。如果社区不相信代表它们的节点，或者感觉网络内的权利太过于集中（或者集中程度不够），社区能够通过集体的改变他们网络内的信任关系来集体移动网络内权利的平衡。

节点订阅关系可以是随机的，并且/或者通过信任网络形成（订阅你知道的人以及社区内你信任的人的节点）。

当一个节点从一个它订阅的链接收到一个新的区块，它发布区块所发布的哈希值。这是一种对接收到区块的公开确认。每个区块加上时间戳并且计数器引用了来自其他链的区块。这创造了一个密集的区块互认的互联链。这些链建立因果关系并且可以作为一种如下节所述的分布式的时间戳系统。这使网络可以证明数据并没有存在，或者没被发布到网络过，或者证明那个特定节点在某一个特定时间间隔内曾经活跃过或者离线过。

当前的Obelisk共识算法基于Ben-Or's随机化共识算法。

一个在随机图中的Sybil攻击（最坏情况下）使得Sybil节点可以控制共识，但是节点不能撤销交易，从而移除了攻击网络的唯一的经济上的激励。在现实世界的图中，网络的Sybil抵抗能力实际上是非常高的，并且运行一个节点在带宽上成本是比较高的，这防止了大的僵尸网络出现。

信任关系是稀缺的，并且可以被撤销。在发生攻击事件时，网络通过断绝到可信度低的节点的链接，并且缩小到一个较小的信任节点核心来进行反应。每个节点的个人区块链留下的公开记录使它非常容易来确认参与攻击的节点。随着攻击节点被识别出来，每个人可以限制和这些节点的关系来降低他们的影响。

- 喵爪币共识是民主的，并且节点由社区来运行
- 喵爪币节点共识是公开的
- 每个节点对于社区和第三方审计是可问责的
- 喵爪币共识系统内的影响是民主和透明的 （但是不平等）

简单的二进制共识算法：在两个区块内选择

每个投票决定是一个哈希对（A,B）。A是父区块的哈希，同时B是区块的哈希。
每个节点对它认为应该是共识区块的下一个区块投票。如果它所订阅的40%的节点具有同样的共识候选人，节点改变它的共识到那个区块。节点在候选人间随机跳转直到达成共识。

一个更高级的系统发布(A,B,P),其中P是从0到1的值。block的所有后继者的P值之和为1。这可以实现多个链分支上的并发共识判决。

如果网络内绝大多数节点是诚实的，他们也将收敛到同一个共识。

喵爪币同时具有一定形式的股份证明。我们投票偏向于具有更大交易费用的区块。

如果对于给定的父区块和包含你的交易的区块只有两个可能的共识选项，无论两个区块中的哪个被网络选择，交易将被有效执行。

撤销一个早期共识决定的概率随着区块深度指数衰减。

共识的高级课题

通过构造网络链接邻接矩阵，我们可以计算测量每个节点影响度的特征值中心量度。我们可以把图聚类并且找到有影响力的子集群节点，然后从子集群中的节点采样从而决定全局共识是否已经达到。

算法的有效性随着每一轮中网络必须从中进行选择的区块数目递减。我们可能使用工作量证明，没有奖励并且难度重新调整控制引入新的候选区块速率。

如果我们可以保证每个判决周期内单一区块，共识会变的很琐细。我们可以在每一个共识周期内引入总体排序，并且只保留顶部区块。举例：在上个区块之后15秒内发布的具有最高转账费用的区块。没有办法完成一个精确的，公平的，每个人都同意的分布式时间戳，但是任何构建总体排序的方式都能工作。

另外一种方法使用一个“公平”的区块彩票方式来选择将挖掘下一个区块的节点。它必须利用图结构来使得受信任的人而非sybil攻击节点获得区块开采权利。如果你有全局图并且为每个节点复制所有链，它是非常容易构建的，但是仅仅利用每个节点的本地信息则将非常困难。

在另外一种框架中，你使用公式来投票成立一个节点委员会来挖掘区块。挖掘下一个区块的权利在一个选举出来的节点列表中循环传递。一旦系统运行起来，你可以尝试不同的方法。节点可以被编程来自动通信和回应。用户可以更新他们节点的程序来把懒人从选举出来的区块矿工委员会中自动剔除。如果足够多的节点添加了那个脚本，它就变成一个强制执行规则。

个人区块链表现为可编程行为的投票。每个人可以添加脚本到他们的节点来检测恶意节点并且和它们断绝联系。网络可以本地化的对攻击获得免疫，通过每个用户选择在他们节点上运行的脚本的行为，而不是采用来自开发者的中心化分发。
我们对于理解个人区块链存在的可能性的理解还处于初级阶段。

攻击类型:

有四种类型的攻击方式:
- 区块共识的判决被主导 （潜在的拒绝服务）
- 撤销之前已经达到一致的共识（双花）
- 延迟共识（拒绝服务）
- 通过控制网络的视图来攻击单独节点

控制网络内绝大多数影响力的攻击者控制了网络的共识判决。然而，他们并不能轻易的双花或者51%攻击。一个控制了网络的攻击者可以对仅包含噪声而没有任何交易的区块投票。

这种行为能轻易的被检测到（公开行为）并且如果他们变的有破坏性，可以轻易的被节点禁掉。

为了撤销共识，需要绝大多数节点变的恶意和勾结。恶意的大多数必须离线，允许整个网络来到到一个特定的共识，然后恢复和其它网络的通信。任意包含绝大多数攻击节点连接的节点将会成功带入一次51%攻击（原始形式）。尽管如此，如果攻击节点少于绝大多数，这种努力将会失败。

这是撤回交易的唯一方式。这是唯一的攻击并且非常容易被检测到。受信任的节点快速切断和攻击节点的联系。牵扯到攻击内的子图很有可能被密集的链接一起，并且不如紧密集成的子图一样大的影响网络。简单的拥有绝大多数节点并不足以撤销共识。一个攻击者必须控制了控制绝大多数稀缺节点和信任关系的节点。对于Sybil攻击机器人，聚合人类的信任网络具有一定难度。

在信任图网络中，影响力是和被社区信任的节点高度联系的，并且由Skycoin股权持有者控制。绝大多数受信任的社区成员和机构能从中获利，或者甚至组织起一次成功的绝大多数影响力攻击的可能性是非常低的。

即使Skycoin下的双花难度很大，仍有可能分别通过两种方法来完全防止攻击。第一个方法是严格限制投票判决的方式，来极大的增加节点间勾结的难度。第二种方式使用分布式时间采样来识别攻击节点。

攻击单独的比特币节点：比攻击网络更容易

每个比特币节点容易受到控制网络路由器的攻击者的控制。这种攻击可以插入重置数据包并且控制节点可以连接到谁。受害者节点可能被陷入双花攻击并且通过分叉单个节点的区块链来窃取币，而不用攻击整个比特币网络。随着比特币的价格上升，这些攻击变的可能性更大和更有利可图。

喵爪币引入了一种“共识预报”来保护银行和交易平台防范在特定节点上的目标攻击。喵爪币共识预报采用一个用户选定的信任节点的公钥列表并且根据列表进行验证。结果的不同会触发一个警告提示用户该行为的存在以及防范措施，比如在资金被窃前暂停交易平台提款。

采用分布式判决状态机通信的公开可验证的可信性计算:

我们描述了一个系统，每个节点公开执行一种计算。该计算能被任何第三方验证和重复。这个系统由通过公开广播频道（私有区块链）进行通信的确定性状态机构成。

发布在区块链中的共识结果变为确定状态机的输出，它的输入为公开数据。我们要求，由一个节点在区块链中发布的输出，是一个由它所订阅节点区块数据的确定性函数。任何第三方可以下载一个节点的公开输入并且验证输出和由节点产生和发布的（区块）输出精确匹配。

这种方法被开发用于并受到关于对抗性Paxos的研究的深刻影响。我们将公开广播频道上的Paxos实现称为“Public Paxos”。

一个第三方审计可以产生一个数学证明，并能被第三方独立验证，不诚信节点欺诈证明。这类欺诈可以被禁掉并且导致信任关系的自动撤销。

这类系统的一个实际实现要求：
- 一个状态机的实现或者定义良好的虚拟机
- 要求每个区块包含一个有信任关系节点的列表的哈希
- 要求正在运行状态机程序的哈希，决定了它的输出（产生区块）
- 要求在反馈中发布从节点所获得区块的哈希

我们采用包含一些很少改变的固定信息的数据结构来增强个人数据链，包括状态机的订阅列表和程序源代码。节点发布它的订阅列表的哈希和每个区块中的虚拟机源代码，并且发布它的订阅列表和程序源代码。

举例：

节点A被节点B和C的私有链订阅。B挖出区块B1。A接收到B1。A发布一个区块，包含了B1的哈希来表示接收到数据。由A产生的区块A1是一个B1的确定性函数。C发布区块C1。A发布区块A1，在它的区块确认列表中包含了区块C1的哈希。A2产生，发布并签名区块A2，必须包含B1，C1的确定性函数。

备注：
- 所有输入是公开的，并且对第三方可查的 （信息发布在一个公开的广播频道）
- 每个节点产生的输出是公开输入的确定性函数

- 任何第三方都能下载同样数据，执行同样程序并且和节点自身生成同样的输出
- 用于产生输出的状态机的状态可能是由节点确认的最近1024区块的队列

概述：
- 你有N个状态机
- 每个状态机通过一个公开广播频道通信
- 每个机器的状态是从其他状态机接收到信息的队列
- 每个被引用的状态机产生一个发布在机器公开广播频道的输出区块
- 输出区块包含接收到信息和数据的哈希 （收据）
- 对于有限N，输出区块是最近N个区块接收到信息队列的一个确定性函数

在这个系统中，节点是高度受限的。节点唯一的回旋余地在于摆弄所确认消息的顺序。一个节点在不被检测到情况下可以参与的攻击类型是严格受限的。

关于分布式时间戳的想法：

最简单的分布式时间戳服务是一个受信任的具有已知公钥和一个精确时钟的中心服务器。服务器接到到哈希并且用它的私钥对哈希产生一个签过名的时间戳。如果服务器可以被信任，签名时间戳能被用来证明数据在某一个特定时间存在过。

精确的，可信任的数字时间戳有很多应用。它们能被用来决定一个节点在某个时间是否在线，他们可以用来检测和消除那些要求先扣留数据一段时间，然后再突然公布数据到网络的特定类型的攻击 （比如比特币51%攻击） 并且能被用来建立区块的总体排序。

比如，使用一个可靠的时间戳服务器的分布式区块共识是很琐细的。规则“接受在上个区块之后15秒内产生的具有最高手续费的区块”可以获得区块共识。这个规则唯一的确定了一个唯一的后继区块。事实上，如果一个精确的并且诚实的时间戳服务存在的话，那么这个简单的规则可以不使用挖矿和在非常低操作成本下产生一次51%网络攻击。

原始的Obelish设计是基于构建一个分布式时间戳，但是仅仅在完全连通图中才能工作。仅仅使用对每个节点可用的本地信息，没有分布式时间戳系统能实现可被证明的在网络中所有节点中发生事件的总体排序的共识。每个节点仅仅看到网络的一个子集。比较小数目服务器的完全连通情况是每个节点都有“全局”视野并和其它节点最终到达相同数据和共识的一个特殊情况。公开广播频道和完全连通图让拜占庭将军问题相当琐细。

由于从每个节点可用的本地信息不能实现时间戳共识和完全的时间总体排序，对非病态的拓扑结构图，随机化共识可以从本地信息提供可被证明的全局共识。尽管如此，我们之前能提供一个稍弱一点的结果，使得节点推导出网络中事件的上界和下界（一个时间区间）。这些边界对网络中每个节点或者节点子集是本地化的，并且对于检测和防止某些类型的Sybil攻击非常有用。

分布式时间戳：

我们展示了你能如何使用Obelisk公开广播频道，时间戳区块和区块确认收据来创建一个分布式时间戳授权。

我们想要创建一个系统，它允许我们高确定性的证明
- 一个区块的发布时间
- 证明一个节点曾经在网络上活跃和通信
- 证明数据存在过并且在某一个特定时间段发布
- 证明数据在某个时间不存在，或者它并没有被公开发布过

拥有这些信息使我们可以构建欺诈节点的检测系统。我们希望以很高概率确认一个特定节点正在选择性的拒绝消息，创建不正确的时间，属于一个勾结的网络子图，或者是不可靠和不值得信任的。

每个节点被其他节点列表的区块链所订阅。每几秒钟，每个节点发布一个新的区块。每个区块加上时间戳并且包含一个节点自从它发布上个区块后已经接收到的区块哈希(收据)列表。每个发布的区块通过发布节点的私钥进行加密签名。

每个节点一直持续发布时间戳区块并且发布由其他节点发布区块的收据。这形成了一个密集的，互连的时间戳，收据和计数器收据的网孔，并且使得它很难被恶意节点回溯事件而不被检测到。

公开广播频道强加了几个约束：
- 一旦发布一个区块，它不能被取消发布 （区块被点对点的复制到所有订阅者。一旦一个区块已经被发布，它将扩展到所有订阅者。你必须销毁所有已经接收到区块的节点来从网络上擦除它）。
- 一个节点不能发布一个之前区块的不同版本而不被检测到 （区块被编号并且如果节点使用同一个序列号签名了两个不同的区块将被检测到）

- 在不延迟区块发布情况下，一个节点对于接收到的区块不能回溯时间戳 （时间戳仅仅增长，时间戳随着区块序列号单调增加）
- 链中的一个区块不能在不报废之后区块情况下被修改 （链接的时间链，每个区块头部包含之前区块的哈希）

情况：

A发布了一个区块。B发布了一个带有A发布区块收据的区块。然后A发布了一个带有B区块收据的新的区块。

节点A被节点B订阅。节点B被节点A订阅。
举例：
节点A发布带有时间T1的区块A1
节点B接收到区块A1
节点B发布带有时间T2的区块B2。B1包含区块A1的哈希。
节点A接收到区块B2。
节点A发布带有时间T3的区块A3。A3包含区块B2的哈希。

这称之为“2-cycle”。如果A信任它们自己并且相信它们的时钟是诚实的，那么A知道区块B2存在过并且在时间T1和T2之间发布。

如果B2在T1之前发布，那么B2不能包含A1的哈希，因为A1在那时还不存在。靠运气猜中哈希的概率是1比2^256。

如果B2在T3之后发布，那么A3不能包含B2哈希，因为A3不能包含在A3被创建时还不存在的一个区块的哈希。

因此B2必须在A1被发布之后被产生并且在A3被发布之前。因此如果节点A的时钟是精确和诚实的，B2在时间T1和T3之间被创造和发布。

因此，这种构造让我们可以依据节点A的时钟来确定性的证明事件在某个时间间隔内发生。在收据图中有更高的cycles，3-cycles，4-cycles等等。这建立了一种通过计算时间间隔的分布式时间戳系统。

你可以证明，如果一个区块X1在时间T发布，一个cycle起始于一个诚实的节点并且在时间T2终止于同一个诚实节点T2，T<T2。这上确界了发行时间。如果我们有一个受信任节点的时间戳T1的后续区块X0的收据，T1<T。之前区块（X0）的收据的时间戳下确界了X1发行时间的间隔。这是利用单调增加时钟假设产生时间间隔的另外一种方式。

有一些节点是诚实的，并且不撒谎。有些节点试图对时间戳以及消息接收到的顺序撒谎。如在不诚实节点间有一个cycle，时间戳可能是任何值，取决于公开广播频道的约束。尽管如此，如果cycle的接收者包含至少一个诚实节点，那么它就会给时间戳放置一个约束。

假设我们有一个cycle的接收者，A->B，B->C，我们称这两个cycles“互连”。接收者之间的cycles在诚实节点子图内宽广的互连。多个互联的时间戳和收据形成了一个密集的互联网孔。如果你说在时间3存在什么事情，但是直到时间8之前并没有将它发布到网络，网络中的所有诚实节点对你宣布那件事情的区块有时间戳，时间大约等于8。仅仅撒谎和欺诈的子图上的节点才会有更低的时间戳。

收据Cycles对于一个给定节点的时钟建立了一个公平的事件的总体排序：

为了证明一个区块在时间5之前存在，我们可以找到一个通过哈希互相引用的区块序列，X1 -> Y1 -> Z1 -> X2。如果区块X2由一个时钟精确的受信任/诚实的节点发布，区块X2上的时间戳上确界了Z1发布到网络的时间，即使我们不相信发布区块Y的节点或者发布Z的节点。

选择一个节点X。我们希望根据X建立一个区块的时间排序。我们枚举所有起源于X的cycles（假设一个loop的cycles，起始于X并且终止与X，并且不多次经过X）。每个区块将被包含在一个或多个起始并终结于X的cycles中。对于一个特定cycle，我们说根据X一个区块的时间是终结cycle的由X产生的收据的时间。对于每一个事件，我们选择具有最低终结时间戳的cycle，对于每个cycle则是包含该事件的最低。

所以如果我们有cycles
X1 (t=1) -> Y1 -> X2 (t=3) (cycle起始于区块X1，终结于区块 X2, x1时间戳是1, x2时间戳是3)
X1 (t=1) -> Y1 -> Z1 -> X3 (t=5)

其中，
- Y被X订阅

- X被Y订阅
- Z被Y订阅
- X被Z订阅

我们有cycles X->Y->X and X->Y->Z->X.

X产生区块X1，时间戳t=1。在区块Y中有区块X1的哈希，以证明Y接收到该区块。

X发布X2包含接收到Y1的收据（其中包含X1的收据）
Z发布Z1包含Y1的收据
X发布X3（时间戳t=5）包含Z1收据

在本例中区块Y1被包含在X的两个cycles中。如果我们信任X的时钟，那么我们知道Y1曾经在t=3之前存在和被发布 （我们选择两个cycles中较低的）。如果Y1是区块Y0的后继，那么我们可以降低Y1发布的时间到X确认Y0的区块时间.

对于可以通过起始于X的收据链到达的任意区块，这产生了一个时间的上确界和下确界。对于一个well conditioned图，这将近似包含所有区块。对于区块发布时间的上确界，我们选择任意cycle终结时间的最小值。对于下确界，我们选择前置区块cycle终结时间的最大值。

我们可以泛化“依据节点X的时间”这种表示方法到网络中一个受信任节点的子图。我们选择网络的一个子集。我们假定网络内的节点有同步时钟并且精确报告时间。我们允许一个“cycle”起始于子图中的任意节点并且终结于子图中的任意节点。

如果节点每十五秒或者每分钟发布区块，我们能有信心把一个时间的时间间隔限定在一个合理大小的时间间隔内。我们可以展示事情在一个给定时间要么没有存在，或者没有发布到网络内causally可访问的部分。

在一个N个节点的随机图中，每个节点的区块时间是一个常数k（比如说15秒），假定仅有一个受信任节点，一个随机事件能够可靠的被解析的时间间隔，具有一个增长的上确界k*log(N)。

消除51%攻击的方法：

分布式时间戳系统甚至能够被用来防止绝大多数节点进行的51%攻击，仅仅通过拒绝和断绝和已从网络断开的节点的关系，并且保证在宣称的时间，对于之前被证明过不可被发布到网络的区块，重新出现可被证明的回溯共识决定。

类似的，对于剩余连接到的网络，不需要正当理由，节点能变得自动不受信任并且自发决定尝试撤销之前建立的共识。

在比特币经典的51%攻击中，一个具有绝大多数算力的矿工分叉了区块链，并且秘而不宣。矿工秘密的超过网络并且突然发布他自己更长的链。网络立即切换到攻击者更长的网络上。交易被撤销并且币可能会已经被从交易平台窃取。

邪恶矿工充值比特币到一个交易平台，买了莱特币，提取莱特币并使用51%攻击来撤销充值交易以重新获取他的比特币并且同时保留了莱特比。之后当盗窃事件在媒体发布后，他使用莱特币来便宜买回比特币。矿工甚至可以买空比特币来进一步扩大他的收益。邪恶矿工同时决定来抢劫一个银行，通过存入比特币，提取比特币并且然后撤销充值交易。他现在同时有了提取的币以及他从未充值的币，只要银行没有采取极其困难的安全措施。

在喵爪币中，分布式时间戳系统允许每个节点来本地化的决定之前一个节点是否在51%攻击尝试中通过对网络隐藏信息然后突然发布。每个节点本地评估信息然后选择是否忽略潜在恶意节点的影响。通过这种方式，在随机图中一次成功的攻击要求超过80%到90%的有影响力的网络节点，而不仅仅是大多数。诚实的节点可以简单的检测和忽略51%攻击尝试。

假设每个节点由独立的但是不可靠的oracle通知决定全局共识（每个节点采样一个网络独立随机子图的共识），在几个确认后我们可以使进行一次成功攻击的概率任意接近于0。这种方法结合了本地信息和全局网络状态的独立随机采样。本地状态被用来判定和协商共识，并且采样全局网络的子图来概率意义上判决全局网络共识是否已经达到并且检测网络分叉。

区块中对于全局共识的概率知识可以用来决定对较早区块的分叉尝试是否应该被接受。 在原始方法中，如果订阅的绝大多数节点投票赞成对较早区块的分叉，节点将接受这个分叉。

通过全局共识oracle，对分叉的投票被下面的观点所加权，刻意的改变是一个合法过程的结果，指通过网络中哪些节点达成一致（网络仍然到达了全局共识），或者是否一致性在很长时间之前已经无争议的达成，并且这仅仅是一次试图撤销之前共识（如果在活跃节点间全局共识已经无争议之后，这将是不正确的）的攻击尝试。

另外一种可能的方式可使用一种Ben Or随机化共识的混合系统，它基于信任网络来投票受信任主节点委员会从而形成了一个完全互连的公开的Quorum，用来决定区块共识。

我们正在研究几种不同的方式。喵爪币共识将随着我们开发更好的算法和软件框架而改变。

https://github.com/wudaofan/mzcoin

喵爪币支付系统
喵爪币支付系统除了应用在支付上外，还对物联网的探索则集中在教育机器人上能做到机器和机器之间的支付。喵爪币希望能基于区块链，为现有的物联网行业提供一种人到机器或者机器到机器的支付解决方案，实现对物联设备传感器的实时接入支付。同时，也让学生接触到最先进的领域。

我们的眼光很长远，他们看到了物联网真正未被发掘的价值：传感器的数据。正如物联网之父凯文•艾什顿说过的：“物联网价值不在数据采集，而在数据能否共享”

全世界几乎有无限的数据量，而人类在采集世界数据方面并不擅长。因此，人们建立了一个非常低成本的，与互联网相连的，遍布全世界的传感器网络。计算机能够用这些自动化的传感设备获取信息。但我们真正需要的，是在传感器网络中得到整体的图景，这才形成了采集数据的物联网。

当传感器收集了数据后，是否有价值取决于信息是否能够共享。
传感器铺设是物联网的架构基础之一。然而，当今大部分传感器都掌握在私有网络中，只为单一应用服务。这种现状违背了真正的物联网愿景——数据共享。

举几个例子，停车场管理公司为了检测停车位的使用状况，安装了一个大型的传感器网络。这样的基础设施建设需要花费大量的金钱，但如今它却只能用来判断停车位情况，这其中蕴藏着宝贵的数据，可以提供给研究人员参考；有些紧跟科技潮流的水务公司，可能会在水龙头上安装传感器，某些卫生组织希望通过这些传感器追踪洗手的频率，为将来制定政策收集数据，但由于这些传感器的数据只属于这家公司，也无可奈何。

显然在这个过程中，物联网的数据也没有很好的分享到需要的人手中。这一方面是因为公司们没有意识到市场对物联网数据的渴求，另一方面，物联网也缺乏一个很好的分享，交易的商业模式。一些云平台，如Xively，Thingspeak，Thingful支持个人分享传感器数据，但由于没有对数据拥有者的奖励机制，使其不愿意提供良好结构并持续稳定的元数据。

因此我们需要建立一个物联网的全球数据市场，进行数据交易。这时有人提出了一个奇妙的设想：既然是传感器为我们提供的数据信息，我们是不是可以直接向传感器支付费用呢？

2014年，两位瑞士的学者发表了论文《如何通过比特币交换传感器数据并实现传感器自盈利》，其中就提到了这样的设想：建立一个由传感器端，请求端，传感器库组成的系统，在这个系统下传感器可将其测量数据值上传至世界范围的数据市场中，利用比特币区块链进行数据交易。

而这正是我们的合作伙伴快贝正在做的，整合全球IoT数据，实现设备自盈利，建立传感器之间去中心化的“支付宝”，。这家公司开发了一个基于比天空币块链的去中心化的支付系统SPV（Simplfied Payment Verification），通过这个系统，硬件设备或者传感器能够快速加入区块链网络。只需要填写硬件设备传感器的ip地址，即可注册硬件设备。注册后，所有物联网设备都会有一个独一无二的钱包，并用来通过区块链技术接收支付。快贝还将建立一个物联网数据交易市场，使大家可以购买物联网中各种设备和传感器上的数据，并以 P2P的方式保证数据和支付的安全传输。SPV系统不仅有windows客户端，还有iOS和安卓移动端的钱包，可以在移动端方便地管理自己名下的物联网设备和虚拟货币。
想象一下，区块链和物联网结合之后，每个传感器都可以进行数据交易，一个私有的气象监测站下属的空气质量传感器，可以通过喵爪币搭建的平台实时出售当前的空气质量数据，任何人和单位都可以通过应用程序购买它的当前数据查询空气质量，类似耐克等运动应用就可以购买该数据，并为其用户提供无污染跑步路线。

再试想一下，无数的设备、传感器都接到区块链上，机器与机器之间自己沟通，机器自己付账、自动工作。那会是一个怎样的景象。智能硬件最大的问题就是数据共享，区块链正好弥补这一点，卯榫相合，前景巨大。通过区块链，物联网能真正实现数据去中心化共享，“机器——人”的服务共享。让每个人都可以利用这些数据做科研或者改善生活。物联网走向物链网，同时拓宽了区块链和物联网的市场，彻底颠覆我们的生活。
当然，梦想是性感的，现实是骨干的。由于物联网技术的复杂性，上下游产业链较长，再加上区块链的发展、成熟需要时间，走向那个智慧物联网世界还有很长的路。但现在， 快贝已经整合了物联网与区块链技术的相关厂家，共同开发并着手制定了相关产业标准。
在软件开发上，快贝可以把区块链底层开放给学生，学生可以尝试在区块链底层上搭应用。物联网传感器实时数据，包括能源，健康，环境，风力，温度，湿度等各方面的传感器实时数据，使传感器节点支持喵爪币的协议和功能，可以让设备在快贝的去中心化交易市场自动交易自己的数据，并受喵爪币的微付款，这些付款收入属于设备的持有人。

区块链对于物联网的最大意义，在于在海量的智能设备之间建立了低成本的、互相直接沟通的桥梁。同时又通过去中心化的共识机制，提高了系统的安全性和私密性。基于区块链技术的智能合约技术，又将智能设备变成了可以自我维护和调节的独立个体。
优势互补，区块链和物联网的联合，将带来更智能的生活。

喵爪币在喵爪星球及极客豆学院中的应用

喵爪币可以帮助我们众筹一个极客豆学院吗？如果可以，那么我们如何做？

第一步：我们用区块链技术生成一段代码，产生喵爪币。

简单的来说，区块链就是把云计算所构建的集中式数据库，通过去中心化的方式分散存储到整个链中每一个节点，将数据库从集中维护的模式转化为集体维护的模式。如果说云计算是一种“封建集权制”的技术模型，那么区块链所代表的就是一种“人人为我，我为人人”的“共产主义”技术模型。

它的教育理念是“以学生为中心”，运用高科技，按照每个学生的需求和兴趣，提供量身定制的课程。

我们通过喵爪币来众筹建立我们自己的学习教育社区---喵爪星球。线上有社区用户创建的，供学习的玩乐课程表（Play List），线下有极客豆学院。

整个社区用区块链产生的喵爪币来运营。想投资的，可以买喵爪币投资。喵爪币可以用来买课程和学习用硬件产品。在平台上发起项目制为导向的学习项目的，可以接受社区用户用喵爪币的投票，获得一定票数的，就可以上线供其他社区成员学习，Play List的创建者可以自己定义收多少喵爪币。Play List的创建者还可以建立团队为学习用户提供一对一，或去线下辅导。这样可以收更多的喵爪币。

在喵爪星球学习社区里，每个用户和设备都有一个区块链钱包。这个钱包就是用户在社区里的身份，钱包功能除了有收发喵爪币，和看账户余额外，还是一个个人数据的数据库。和今天的中心化数据库不同的是，这些数据的拥有者是钱包的主人。任何公司都不能看到用户数据。除非钱包的主人主动给数据。

喵爪币可以兑换人民币，比特币，小贝壳和天空币等其他加密数字币。

喵爪币可以换天空币，天空币也是一个通讯的手段，而所有这些分享、协作、跟踪、广播、诠释、鉴别都是功能，我们可以通过分享来实现这些功能。人类语言文件和智能合约代码之间创建一个数字链接。这些功能都会实现在极客豆学院的技术后台上。

第二步：极客豆学院--玩乐课程表 （Play List）没有“年级”的另类学校

在极客豆学院，学生签到、考试、完成作业全部需用Ipad以及可穿戴设备进行。学校会让每个学生家长买一台Ipad，一年后换成笔记本电脑。电脑上装有极客豆学院的电子平台mzworld.cn。每周老师都会和每个学生聊天，通过了解他们的兴趣和强弱项，在学生个人帐号中制定下一周的学习计划，约25个新任务列表(Playlists)，列表会清晰写明完成每项任务的具体操作指南。学生用电脑查看任务，完成后在线提交文档或照片至mzwolrd.cn的线上数据库。根据在线了解学生完成的情况，老师可一对一进行辅导并在下次制定任务列表时对学生个人的薄弱项加以强化。

极客豆学院其实并没有严格意义的分班，它在教学过程中把进度相同、兴趣相同的学生聚集在一起做项目。如果这个学生在某一项目上学习速度较快，可跟高年级同学一起学高阶课程，但其他项目仍旧跟同龄人一起上。

在这里，每个学生都有一个学习进程表。表格的横轴上，清晰标注著入系统的成绩，表格的竖轴上是各个项目。学生已经完成了的项目，会用绿色表示，仍在做的学科被标注为橙色。老师可点击任何项目，从而得到进一步更精确的信息。他可以看到学生搜索了多少知识点，以及为这个知识点做了微课没有?

极客豆学院会找最好的设计师和工程师，优化整个技术系统。极客豆学院会利用Wolfram的强大的搜索功能，建立学生可用的知识库。尽管目前极客豆学院的数据库还很小，还刚刚开始，但当有一天，我们有了大数据，我们将会找到方法，完善教育系统。

教学法的设计

极客豆学院用一种混合学习模式取代原来的教师主导式教学，现在学生有“自主学习”（solo time）和“小组学习”（group time）两个学习场景。孩子们花半天时间天的时间沉浸式在线上教育，半天的时间接受传统教室指导，这些全部有强大的数字平台系统做支撑，能够满足学生个性化学习和评价体系的数据量化，家长也能及时在网上了解孩子的学习进程。

孩子们每年还有两周的时间放下一切教学任务，共同去分析同一个社会问题，并尝试提出解决方案，从3年级到高中的孩子们解决的是同样的问题，最终不同的年级都要展示最终的方案，他们的相互间的比较也很有趣。其实，这项教学任务和我们开展的综合实践活动课程相似，但他们的确保证了孩子有充足的时间去研究，而且设计的活动主题是解决社区里真实存在的问题，这让学习这件事不仅变得好玩而且有意义起来。

极客豆学院打造了基于互联网的项目制自适应学习体系，培养学生创新能力。
为培养具有创新能力的优秀人才，我们的教育应当以学生为本，以提升学生综合素质为导向，提倡个性化教育，从而激发每个学生的潜能。 为此，学校应当以教育信息技术为支撑，构建优质学习资源系统和个性化学习平台，创设适合每个学生发展的教育。 为实现这一目标，有效步骤是：

1.充分应用信息技术，根据学生需求推动个性化教学、 通过微课、翻转课堂和项目制学习，来培养学生自适应学习的能力，通过融合学科的项目制学习来推进教与学方式的变革。

2.深化学生成长电子档案数据信息的应用，推进基于学生成长数据的个性化指导和有效干预，通过游戏化机制定制个性化的学习，引导学生创新思维。

3.统筹推进个性化的学校建设、社会资源配置、师资培养、教育评价等，使学生的个性化发展需求得到充分满足。

为此，极客豆学院成立创新实验室，依托互联网教学平台、智能硬件（传感器、3D打印设备、机器人等）设备与实际应用项目的引进，建立鼓励学生以项目为导向的自适应学习、实践，将极大培养和激发学生们的创新能力。实验室将常态化地培育出基于发现和解决社会实际问题的学生创新项目。

极客豆学院将通过创新实验室充分整合和利用社会教育资源，携手教科研单位以及其他学校及社会资源协同创新，为学生营造有效的创新实践生态圈，组织相应创新实践活动，积极鼓励学生走出校园，参与社会实践。让课堂从校园走向社会，丰富学生创造、创新经历和体验，培育出优秀的学生项目。

从长期发展的趋势来看，随着移动技术、新教学模式、和无处不在的互联网之间的不断整合，学生在学校里的角色正在逐步发生着变化：从被动的教学内容和知识消费者转变成内容和知识的创建者。与此同时，教师的角色也将会被重塑：从课堂上知识的灌输者变成教室里的教学研究与开发者、整合者、教学活动的组织引导者、和参与者。

因此，我们需要建立一种机制，用来激励学生获得学习的主动权，开展探究式的深度学习，将各学科相融合，培养学生的复合思维，用多种知识和技能解决问题、完成任务、甚至挑战论证。 因此，在传统学科学习的基础上，打造项目制的学习将会有效培养学生创新技能。在此基础上，基于孩子们爱玩的天性，积极研究游戏化机制在教学中的应用，进一步激发孩子们的学习热情和主动探索式的学习。

综上所述，极客豆学院创新实验室的任务是：培养学生编程与设计思维，以及运用科学技能与素养创造与发明。这一任务，将通过引进项目制学习来实现学生的自适应学习和创新。

玩乐课程表（Play List）

在常规课程以外，留一些时间让学生去做自己选定的项目。让学生主导，从自己的兴趣和热情出发，自己选题、自己找资料、自己研究、自己得出结论、自己把研究成果展现给大家。事实上，这是一种非常开放的 “项目式学习法” （Project Based Learning）。

Play list学习法的特点是:

以学生为中心

不循规蹈矩

自主探索和研究

研究真实的问题

让学生自我选择新的挑战（Play List）

非常个性化，鼓励创意

目标导向

强调协作和社交的作用

Play List学习法鼓励孩子们在项目上的合作，让学生们自由组合，一至三个人一组，自己选定一个题目，我们在网站上有可以让学生去做项目的空间。学生可以自己设定目标和时间表的空间。在每周统一的时间段里，学生以小组为单位，讨论完成自己的项目。

网站的Play List设计做了一下几个步骤

1、让孩子了解基本过程

首先，会有微课或其他形式介绍项目背景。让孩子们知道所谓做项目，就是提出问题，选择研究主题、去做研究、和同伴讨论、分享成果等，非常具体。

本阶段学习的三个重点:

- 你要去研究一些问题

- 你要去创造一些东西
- 你要把项目成果展示出来

2、从兴趣点出发，确定选题

真正的探索和开创性工作来自于一个人内在的热情。PlayList学习法的本质就是教孩子从热情出发，采用好的方法，达到自己探究的目标。

3、做项目规划

确定了自己要研究什么问题后，网站会让孩子去进一步确立自己的项目建议 Project Proposal，对于小学前后的小孩来说，这么简单的一个提纲，就能把孩子的思路理清楚。

- 你的研究课题是什么?
- 在确定这个课题的时候，你给自己提了哪三个重要的问题?

（也就是让学生搞明白定这个课题的思路和原因是什么）

- 为什么这个课题对你来说很重要?
- 你打算从这个项目中学到什么?
- 你打算和其他人合作么?
- 你需要哪些材料?
- 告诉Play List制作人能帮你做什么?

4、有计划、有目标地完成项目

有了项目建议，老师Play List创造者会强调 List的“游戏规则”

- 在Play List里，你必须一直在做你的研究和创作，不能浪费时间
- 如果你需要一些材料，应该事先准备好
- 学生必须把你做了什么、项目进展汇报写在项目空间里
- 如果你不认真去做，老有延误，对不起，List的主人会踢你出去。
- 无论什么情况，请一定按计划、按时完成你的项目

通常的Play List，包含了PlayList的主人和学生一对一的讨论、每周或每两周一次的目标设定及自我评估。这个服务Play List主人可以另外收费。

一个 play list项目可能会要分很多阶段完成，比如，play list的主人可以把一个项目分成多个阶段，给每个阶段定一个目标，确保学生一步步达到目标。

小孩子通过这种 Play List的训练，不光锻炼了自己探索研究的能力，而且养成了不拖延、做事有板有眼的好习惯，是难能可贵的成长经历。

5、展示研究成果，Presentation 很关键

presentation 是很关键的一环，研究成果的展现方式一般包括三个部分：作品、文字报告和演讲。演讲中又会让孩子调用PPT，视频，幻灯，图表等多种展现形式，全方位展现自己的研究成果。

我们会在各地做Inno Edu的演讲会，给Play list的创建者和学习者一个舞台去展示自己。还会给好的Play list 做工作坊的机会。

6、项目结束，平台评价打分

最后，平台还会对项目完成情况打分评价，一部分是针对项目成果展示（Presentation of Project）的评价；一部分是对学生在做Play List表现的评价。评价是社区投票来评价。

总之，Play List的核心在于这是一个让孩子发挥主动性、创造性，从自己的兴趣点出发，去深入学习、思考、研究、探索、创造的过程。这个过程中，孩子学会了怎样把一个想法变成现实，还成为了更好的阅读者、写作者、沟通者和倾听者。

具体项目

1. 智慧农业项目制学习教学规划及实施步骤

一、核心问题

基于食品安全，环境保护等真实问题的项目化学习

二、研究目标

通过解决食品安全，环境保护等真实问题的融合学科项目化学习，引导发展学生的三大学习能力，从而培养学生的学习基础素养，并且达成学生社会化能力的发展。

三、研究内容

智慧农业学生项目：通过计算机信息课与科学课的多学科融合，让学生学习Scratch编程及相关智能硬件的运用，引发学生对于食品安全、环境保护等问题的思考，引导学生利用

scratch技能找出解决问题的方法和可能性，以此延伸至学校绿色种植大棚的实际操作和研究，培养学生的以下能力：提出问题解决问题、建立合作联系、个性化表达，激发学生自我学习、自我研究的兴趣；结合后期的商业思维培养和创业培训，通过与校外企业机构的合作使该项目落地，培养学生社会化能力的同时，也进一步研究和摸索出更适合学习基础素养培养的教学模式和方法。

四、实施步骤

第一步　计算机信息课Scratch编程教学，结合进一步的智能硬件教学，培养学生对Scratch技能的掌握和熟练运用；

Scratch是由美国麻省理工学院媒体实验室(MIT Media Lab)设计开发的一款面向儿童的简易编程语言。适合于青少年的程序设计教学和最初接触程序设计的人们，借助内置模块设置，通过简单的拖，移，放的动作，完成程序编写过程。支持开发电脑游戏、互动故事、图形艺术作品、电脑动画等多媒体作品。涉及计算机科学、工程、语 言艺术、数学、音乐、科学、社会课程、教育、技术和视觉 艺术等学科领域。未来社会是个物联网的世界，学会使用传感器十分必要。Scratch结合传感器的教学，可以给学生们设计、开发、探索编程以应用。

同时，利用在线平台资源将课堂进一步延伸。对学生：用有趣互动的任务和挑战的方式，让学生们主动探索，自己定义目标，寻找任务及获取信息，促使他们在学习的过程中，开发更多的创意。在动手创作的过程中提高解决问题的能力。在和伙伴互动交流分享的过程中，提高沟通和团队协作能力
对老师：为不同学校不同专业的老师搭建沟通和分享的网络，资源共享。把老师从简单重复的教学中解放出来，更多精力投入任务和挑战的设计，以及根据不同学生的特点困难进行有针对性的教学，体现教育因人而异
对家长：从简单督促学生学习转化成更多个性化指导,并且不用担心孩子在网络的安全

同时科学课提出食品安全、环境保护等具有普遍意义的社会问题的研究与探讨，引导学生自主思考，并实际运用scratch技能得到解决这类问题的方法。根据学生提出的各种初步想法，引导分组讨论，提出项目设想，培养学生的建立联系和个性化表达能力。

第二步　学校建立绿色智能种植大棚，引导学生利用Scratch技能与智能硬件运用知识，跟踪采集植物相关数据并作研究分析，期间引导学生分工合作学习能力，同时培养学生的实践操作能力。

第三步　植物成熟采集期，引导学生利用采集的植物数据做食品安全研究报告，引发学生对食品安全和环境保护等热点问题的思考和关注，并发展学生自主思考、提出和解决问题的能力。

第四步　商业思维培养与创业培训，引导学生分组讨论，让学生自主思考真实的社会问题，并且得出解决方案并成立相关的项目公司，制作对应的商业计划书，以培养学生的分工协作能力，社会化意识和责任感。

通过项目路演的方式，将收获的植物或农产品以售卖或义卖的形式进行发售，培养商业意识的同时培养学生的慈善意识。

2. 智能家居项目制学习教学规划及实施步骤

一、核心问题
基于雾霾、空气污染等真实问题的项目化学习

二、研究目标
通过解决环境污染，实现家居自动化等真实问题的融合学科项目化学习，引导发展学生的三大学习能力，从而培养学生的学习基础素养，并且达成学生社会化能力的发展。

三、研究内容
智能家居学生项目：通过计算机信息课与科学课的多学科融合，让学生学习Scratch编程及相关智能硬件的运用，引发学生对于环境污染、家居自动化等问题的思考，引导学生利用scratch技能找出解决问题的方法和可能性，以此延伸至解决PM2.5，以及探讨解决地方性环境保护等实际问题，培养学生的以下能力：提出问题解决问题、建立合作联系、个性化表达，激发学生自我学习、自我研究的兴趣；结合后期的商业思维培养和创业培训，通过与校外企业机构的合作使该项目落地，培养学生社会化能力的同时，也进一步研究和摸索出更适合学习基础素养培养的教学模式和方法。

四、实施步骤
第一步　计算机信息课Scratch编程教学，结合进一步的智能硬件教学，培养学生对Scratch技能的掌握和熟练运用；

第二步　引入智能空气净化设备结合感应器何移动终端的探索式学习

课程内容包括：

1. 空气净化的原理

2. 典型的HEPA滤芯设计

a. 前置滤芯

b. HEPA 滤芯的定义还有制作

c. 活性炭层

3. 风扇

4. PM2.5 激光传感器

5. 电路板（Photon）WiFi 模块

a. 手机应用

6. 云端计算

a. 智能传感链接一切

7. 电路版，控制电路

8. 有机的空气循环设计

第三步　引导学生利用采集的数据做专题研究报告，引发学生对环境保护等热点问题的思考和关注，并发展学生自主思考、提出和解决问题的能力。

第四步　商业思维培养与创业培训，引导学生分组讨论，让学生自主思考真实的社会问题，并且得出解决方案并成立相关的项目公司，制作对应的商业计划书，以培养学生的分工协作能力，社会化意识和责任感。

3. 游戏化教育教学规划及实施步骤

一、核心问题

融入学习基础素养的游戏教学，多学科融合教学。通过搭建虚拟工作坊等，实现慈善公益招募资。实现认知化学习

二、研究目标

通过中美学生在沙盒游戏平台——MZWorld上自主搭建现实场景，培养学生的想象力、创造力和团队合作能力；同时基于MZWorld的游戏化场景和任务制学习模式，使学生能够在线互相学习，互相指导交流，实现peer learning，促进学生更加积极、主动、愉快的学习。

同时，通过Wolfram知识引擎，实现认知互动学习。

三、研究内容

通过高自由度的游戏平台——MZWorld，让学生在三维空间中自由地用不同种类的方块搭建学校和所在区域的场景供学生学习； 通过peer learning促进学生自主学习。一方面培养学生的想象力、创造力和交流沟通能力，另一方面由于游戏学习场景搭建前期，需要学生探索和调查学校和周边环境，可以培养学生的合作能力，完成社会调查实践。

喵爪初期赋予学生的游戏化项目包括：1. 上海合众公益园虚拟空间工作坊的搭建和公益项目的实施；2 Wolfram认知平台的搭建和学习 3. 学科类的“我的空间”搭建

教学方面可以通过此研究进一步探索游戏化机制在教育测评和教学中的运用。

四、实施步骤

第一步 计算机信息课，教学指导学生掌握运用MZWorld平台；学生自主分配任务， 在老师的指导下将搜集的场景数据（如教室场景，体育馆场景，开心农场景等）转化成“我们的世界”并熟练运用。

第二步 学生在MZWorld平台上分组自主搭建负责的场景；搭建场景所需要的材料需要在平台上通过完成任务获得，学生可以自主发布或申请完成任务以交换所需材料，完成任务的发布和执行。

第四步 劳技课指导学生自主制作VR虚拟现实眼镜，通过VR眼镜在MZWorld上直接观看学生发布的微课或“我们的世界”，实现真正意义上的在线课堂，达成沉浸式学习的目的，进一步激励学生自主学习的兴趣和效率。

整个游戏的运营都是用喵爪币。

西游Go

是我们开发的一款游戏用于奖励学生的学习。学生完成Play list可以获得虚拟道具和妖怪。这款游戏也是用喵爪币作为游戏币的。

西游 GO

混世魔王不小心偷走了镇压妖怪的经书，关在牢笼里的妖怪都跑了出来，散落在人世间。你致力于恢复世间的和平，要收服妖怪，成为最厉害的西游捉妖师，同时散落在世间神仙、佛门弟子可以与你成为伙伴，一起去收服世间的妖怪，这就是《西游Go》。

《西游Go》是基于公司之前开发的儿童汉字教育游戏《西游汉字》自有IP 构建的AR世界，人物、道具和场景设计也均出自其中。 《西游汉字》发布后曾被苹果商店多次登榜推荐，这个主要针对k11儿童的教育App因为独特的玩法设定和可爱的人设，在家长和孩子中积累了大量粉丝，同时积累了很多教育圈的资源。在去年，他们也曾计划西游汉字的AR项目，并做了很多的实验本，但最终由于各种考虑，并未最终立项。我们在去年采访西游汉字项目开发的负责人陈扬时，他曾向我们表示，当时基于卡牌的AR 体验，并不理想，是一个伪需求。但对于AR技术在游戏中的应用前景，却一直吸引着他继续研究。如今 Pokemon Go 的火爆，终于让他找到了他所认可的AR游戏呈现形式。

核心玩法

与Pokemon Go 类似，西游GO 包含四大核心玩法：

AR捉妖：西游妖怪分布在世间，碰到妖怪，开启摄像头，进行AR捕捉，使用宝葫芦、乾坤袋等发起捕获。

妖怪养成：捕获妖怪，通过对战、完成任务等提升妖怪等级和经验值

妖怪对战：玩家间妖怪对战，自己的妖怪与野怪对战。

LBS占领地：玩家组队派妖怪去占领现实世界中的地盘，妖怪对战抢夺地盘。

多样化的玩法

因为多样化的游戏玩法
除了传统的线上游戏运营，依据AR游戏与现实世界联系起来的特点，在运营上也增加了很多可能：

比如和优质连锁品牌合作，推出品牌妖怪，进行线下倒流。就像你可以为了买一个小黄人玩具专程去吃麦当劳，当然你也可能会为了抓一个限量小怪物专程去买个汉堡。事实上，前两天的新闻中就曾有报道，在美国的一家咖啡店，为了增加客流，购买了两个pokemon lure放在店门口，结果吸引来了大量的训练者。

同时，和热门商圈、商场合作，开展周末、节日活动，也是一个很有想象力的场景。如在游戏中发布一个任务，将玩家引导到合作的线下活动。就好像传统游戏中一起下副本一样。但却让真实的玩家走到了一起。Ingress 曾发布数据，说在8级以上玩家中，超过40%的人，因为这款游戏，认识了15个以上的新朋友。并且有超过30%的玩家，在游戏中约会过其他游戏玩家。基于现实世界的联系是线上游戏无法取代的体验。你很难想象，与一个从未见面的人，能形成多深的友情。而AR游戏，却有可能构成一个新的社交场景。

再者和可穿戴设备（手环、智能手表）厂商合作，作为实体道具或交互设备接入游戏，就像Pokemon Go plus。其实，这也是一个很有想象空间的地方。在游戏中，可以构建出多种外设，如过当你购买了外设后，将影响或增加你在游戏中的玩法。这会对玩家构成强大的吸引力。

另外还可以通过周边产品如 西游妖怪AR卡牌、西游妖怪徽章等和游戏形成互动。比如，你可以通过在玩具店购买的卡牌来解锁珍惜妖怪，或者能力培养道具等。并有可能将其作为一种特许经营权，给到想为自己的店面增加人气的零售点。等等。

《西游Go》 借鉴 《Pokemon Go》和《Ingress》 的基础上会增加很多自己的创新元素，并且在玩法和运营上都更进一步。《西游Go》 并非一时跟风效仿，经过多年对游戏和AR

技术的探索，公司很早就在准备西游AR游戏，但苦于当时真的太早，投资人难以想象这个游戏的玩法、很多时候，和投资人说再详细，他们也很难想象游戏的玩法，也根本不相信这类游戏的市场接受度，所以项目迟迟没有推出，而《Pokemon Go》和《Ingress》的火爆印向资本市场证明了这类游戏是有市场的，之前的技术积累，一下子就有了用武之地，使他们能够迅速向市场推出这样一款游戏。

从和游戏结合最密切的点来说，区块链让我们有可能创造出一套更高效安全的数字财产的交易系统。从前我若是想要交易一个数字资产，是非常麻烦的一件事情，需要有类似淘宝这样的中介机构去保证买家能收到钱，卖家能获得他所购买的小精灵。万一买家付了钱，而卖家却没有把小精灵给卖家，那淘宝这样的平台就需要去人工核实问题所在。交易过程复杂，造成流通成本高，因此数字财产无法形成一个大的有效市场。但一旦接入了区块链技术，由于无需中介，且交易容易被验证，且公开透明，一个数字资产的市场将有可能会形成。玩家或非玩家，都将能够像在如今的期货或股票市场中投资交易游戏中的道馆，和小精灵。

你玩游戏时形成的数据，也将有可能能为你自己创造收益。比如，我平时常去哪一带抓妖怪，路过哪里，在游戏中消费了些什么。之前，这些数据都在游戏公司的手上，这些数据都有可能是潜在的金矿。而若是游戏公司利用这些数据获得了什么收益，也与你无关。况且由于为零散的数据寻找买家，商务成本太高，效率太低，很难形成有效需求。而区块链技术的引进，或许能让你的游戏数据，为你自己产生收益。由于数据公开，且可验证，今后，需求方，或许只需要在软件上查找我需要的数据类型，就能够购买到相关的数据，并且，收益会根据智能合约自动进入你的喵爪币账户等等。

4. 3D设计课程

3D打印技术引爆工业4.0，位居未来20年世界大国科技战略之首。如今创客界，最新最酷最火非3D打印莫属。美国几乎所有大中小学已经开设并不断丰富3D打印创新设计课程。3D技术被视为中美制造业竞争的最重要砝码，正加速被广泛运用于工业生产、医疗建行、时尚生活、创新教育等各个领域。

同时，设计思维是非常重要的教学内容。将设计与3D相结合，给出工业级的设计思维培训，对于创业技能培育至关重要。

将用于创新项目制学习的3D设计课程具体课例，列举如下：

1. 传感器产品外观设计及打印制作
在智慧农业、以及智能家居项目中，将其中部分传感器产品开放给学生，允许他们自行设计、打印制作已完成传感器产品制作。

2. 慈善公益产品的设计及打印制作
作为项目的延伸，允许学生利用智慧农业、智能家居项目或自行设计、打印其他产品，参与MZ World慈善公益项目。

3. 全球小发明家（Global Inventors）
“Global Inventors”课程是以学生学习如何运用科技创新创意设计思路和方法进行创新发明，服务周边的人和事物，深受中外学生喜爱和科技创新创意教学界名师名家的认可。“Global Inventors”课程中，学生将学习有关著名发明家及其发明作品，了解他们如何在失败中成长。在每堂课上，学生将学习如何使用3D打印机与电脑辅助设计软件，通过和国际教室的小伙伴联线，共同完成创作发明成果，分享自己的学习经验。“Global Inventors”课程不但可以帮助学生提升3D打印相关知识和创新创意设计能力，也可以培养学生国际交流、协同能力。

4.自动驾驶汽车项目
帮助学生使用照相机、雷达感应器和激光测距机来“看”其他的交通状况，并且使用详细地图来为前方的道路导航。

在IBM Watson的机器人平台上，搭汽车大脑，可以在车里可以用语音告诉用户需要知道的一切信息。

学校创新中心主要板块：

--Scratch活动区：
- SCRATCH相关知识学习；
- 传感器的学习
- 作品的设计和创作

2. 机器人活动区
机器人项目的学习与活动区域

3. 3D打印，激光切割机、机床
通过将3D激光扫描仪结合3D 打印机的手段，小朋友头脑里的大部分的想法可以得到实现，而不是仅仅局限于想象或虚拟世界。

－进行3D打印机，3D扫描仪，激光切割机，机床等先进工具的使 用学习和操作实践
－ 了解科技制作中其它基本工具和仪器的使用并实践

4. 视频制作、录音制作

视频制作等是学生们完成多媒体作品创作必不可少的一部分。有助于完成最终项目及作品的呈现。也是当今信息技术深度应用于教学中的必要需求。基本设备包括：摄像机、小型调音台、话筒、三脚架、电脑、刻录机、声卡、隔音设备、监听设备等。

5. 主活动展示区：
学生可以展现自己创作的成果，也可以从他人的想法中汲取灵感和启发。

极客豆学院重新定义教育，通过沙盒游戏组建一个学习型社区，让不同年级的学生互相辅导。
同一个班里不同学生上的课程不同。譬如：一个擅长数学的3年级孩子可能在上着5年级孩子该学的数学课，而阅读课仍然与他同龄的孩子同步。这样一来，每个孩子都能发现自己有不如别人的地方（弱项），但也有比别人做得好的地方（强项），他们也许羞于向老师提问，但很乐于与同伴一起解决问题。
再譬如，即使围坐在一起进行阅读训练，每个孩子的学习方式，和要求的学习成果也是不同的。譬如，对于阅读水平已经很高的学生，老师会要求他将文章改编成剧本，或做改写。而对于阅读理解能力尚需帮助的学生，也许只是回答几道互动问题。
在这里，填鸭式的教育模式被否定，学生被鼓励，不单单做一个问题解决者，更是一个问题发现者（not just be a problem solver, but a problem seeker.）
在这里，小小孩用平板电脑，而大一点的孩子用手提电脑，他们通过电子产品来完成定制的课程、项目和活动。老师每天会在游戏里将当日的任务发送到学生的任务单里，活动也许包括在MZ世界里做20分钟数学，或者与同学合作创造细胞的一部分。学生完成任务后

提交后，系统会自动评估学生的学习。这样，老师可以为不同的学生布置不同的功课，于是离因材施教又进了一步。

在创新学习正式开始前，老师会和学生聊天，以期勾画这这个孩子详细的学习者档案。此外，老师会把一些数学、语言问题给学生，但他们做得对错并不重要，重点是老师需要更了解学生本身的性格癖好。

由此，学生档案里，除了基本的个人信息，还有他们的兴趣爱好、学习方式、强项和弱点、个性偏好等等。这些档案成为我们为学生制作个性化学习计划的依据。依靠软件的帮助，老师会根据学生现状来制定全年的学习目标。这些目标最终细化为每周都会更新的游戏清单（playlist），学生每天在这些清单上挑选不同的项目学习。当这些清单完成，意味这他们掌握了一项项的学习目标。

也许颠覆教育的最初动力来自他自己的孩子，但现在却更坚信，用技术手段帮助孩子自我学习、自由探索，这才是属于未来的教育方式。

MZ World：沉浸式体验学习

MZ World的创立愿景，就是培养孩子们的创业思维和企业家精神。有了创业的能力，这些年轻人未来能更好地去发现和解决社会中存在的问题。

MZ World帮助他们学习有关创业、经济和社会的“沉浸式体验学习”。主要通过沙盒游戏方式，将在校所学的知识，运用到模拟的社会中去。

那是一个让小朋友们体验不同职业的商业项目。那么更真实地让小朋友学习他们在社区中的角色，以及了解社会是怎么运转的教育项目。

进入MZ World前，小学生先在网站看微课。微课话题涵盖社会、经济、商业、创业等领域。

课堂学习后，学生们就可以进入沙盒游戏，进行模拟体验式学习，尝试将他们所学到的理论知识运用到现实生活

例如，小朋友3人一组，设计一项服务或产品，并设法申请获取投资机构的启动资金，然后通过各种营销手段出售自己的服务或产品；拿到盈利或工资之后，他们便可以根据自己的需求，买入别人的产品，继续拓展业务，或转而做其他的投资。
MZ World有一套自己的用区块链技术的金融系统，因此，所有成员的开销、流通产品的购买价格、销售状况、工资水平等各项数据都会由IT团队在后台进行实时更新。在项目之后，孩子们通过这些数据，可以清楚地了解“物”和“钱”是如何在政府、个人和企业、非营利机构等间流动的，从而更直观地了解社会的运作。
这种并非以单向的授课方式来完成教学大纲的任务，而是把大纲融入角色扮演和更广的社会范畴里的尝试和成功，再一次验证了，只有当孩子们发现他们所学的知识能够真正运用到现实生活中时，他们的学习兴趣才会被提起。

第三步：建立线下未来的学校的空间
如何设计，才会成为学生自由成长的“生命场”？

如何为未知而教，为未来而设计？
如何打破传统校园的设计概念，让校园不仅仅是学生学习、做作业、上课的地方，而且是孩子觉得好玩有趣的，充满学生味的，生态的，有生命力的环境？

NO.1 未来教室

开阔的教室空间
偌大的落地窗
把自然光毫无保留地引入室内
教室摇身一变成为展示交流空间
在这里自主学习空间

支持系统的设计

极客豆的支持系统，主要分为三部分：
1 学习进度跟踪；对于每个学生的进度，极客豆学院都会实时跟踪，并根据这些数据帮助孩子们个性化学习；
2 个性化教学工具；Playlist 允许每个学生定制化学习内容，并根据自己的兴趣选择适合自己的课堂。
3 家校沟通平台；基于数据，家长们更了解学生，因此更为深入参与到孩子们的成长中。
极客豆学院可以提供多种不同的个性化学习方案，之所以可以做到如此，就是强大的科技和数据支撑。

极客豆学院，只是最早的一个发展形态。这是一个“长期”的过程，而现在所做的是一种典型的“硅谷创业”模式，先在一个小范围内创立，发展和完善产品，而最后 极客豆学院想要做的是基于共享逻辑建立生态。
在“线上建立项目制自适应学习生态的尝试”之后，极客豆学院 的下一步是“帮助教育者开办学校”，我们正在推出自己的个性化学校管理系统 —— 任何人都可以向 我们寻求合作，建立个性化班级以及学校。付喵爪币就好。

学校之间的组织形式也不会再是从上至下的组织形态，而是一种网状结构，每个学校都是不同的个体不同的点，其相互连接相互分享。这样所构成的网状结构是一种新的学校系统，系统化的创造价值和共享，而这就是“个性化学习生存的土壤”。大家用其他用户创造的内容，要付喵爪币。这时的互联网不仅是信息的互联网，还是价值互联网。
但是，并不是使用了极客豆学院的后台就是复制了一个新的极客豆学院，我们认为每个学校都可以采用他们个性化的学习系统，但这不代表失去了学校本身的教学理念和方向，个性化教学是一种方法而不是一种思想。

未来，大量的公立学校也将接入喵爪币的学习生态系统，与所有的教育者共同分享教育+科技带来的突破。

我们将发行3亿个喵爪币，然后不再增加发行量，跟法币，人民币和美元币比，优越性在于不会贬值。喵爪币的获得会有两种途径：1.用人民币买。2.创建Play list，接受喵爪币的投票。在投票过了以后，上线运营后接受用户付币学习。3.在学习过程中，赚取西游Go的妖怪，养成以后卖掉换喵爪币。喵爪币会在交易所上市交易。用户可以换人民币，比特币，小贝壳和天空币等。

这会是一场社会实验，志同道合的人们会用喵爪币一起来构建一个学习社区，这个社区的融资，内容的建设，学校校院的建设都将用块链创造出来的货币来解决。在互联网时代，社区只是一个信息传递的平台，在区块链时代，社区是个价值可以很容易转移的时代。

现在许多人在抱怨，学校教育不能让他们的孩子成为创新者，然而也觉得没办法，大环境就是这样。那么，这是一个伟大时代，我们的孩子们将会在区块链，人工智能，物联网，3D打印以及AR，VR的技术环境里生存，如果没有创新能力，是无法在社会里生存的。我们认为，自己的孩子自己养。让我们一起来用喵爪币，众筹一个Alt School式的为每个孩子定制的，以项目为导向的自适应的学习社区。

喵爪币是我们创建一个学习社区，一个自组织的介质。它给我们一个机会来重构教育。我们会因为一个区块链技术产生的喵爪币来改变世界。