# BTLink 公链白皮书

V1.0

BTLink 是 web3.0 区块链互联网协议的运行 BTL 的公链，包括使用链上数字资产，来代表定制货币和金融工具（彩色币），某种基础物理设备的所有权（智能资产），如域名一样的没有可替代性的资产（域名币）。BTLink 公链逐步运行上线官方商业生态:DEXswap，NFTswap 去中心化交易所，去中心化的金融衍生品，game finance2.0-3.0 链上游戏，social finance 去中心化社交金融，read mining 阅读挖矿，metaverse 元宇宙，Loan finance 借贷金融，Insurance finance 保险金融，blockchain mall 区块链商城，machien gun pool 机枪池，二维码嵌入钱包地址，BTL+各国数字货币挖矿 BTL，点到点博彩和链上身份和信誉系统，开放接口全球商业对接等更高级的各种商业应用。

BTLink 另一个重要领域是“智能合约”，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扩展，就是去中心化自治组织（DAOs），-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。BTLink 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。如可编程的去中心化金融，去中心化的借贷协议，去中心化的保险协议，去中心化社交协议，去中心化的链上游戏，去中心化的交易所，去中心化的贸易协议，去中心化合同协议，去中心化的财务管理系统，去中心化的工资绩效协议，去中心化的各种 DAPP 应用，就能够创建以上提及的所有系统，以及许多我们都还想象不到的的其它可发明，可创新，可创建，可编程的各种系统。

BTLink 的公链原生数字资产，BTL 通证的发行方式是划时代的。它颠覆了比特币、以太坊等所有的公链数字资产的发行方式，按通证每次市值上涨的百分比参数，发行相应 BTL 通证的数量。如已发行的 BTL 通证市值不上涨，剩余 BTLink 公链上的 BTL 不发行，没有像其他公链资产每天发行，每天不断形成越来越多的抛压。已发行的 BTL 存量的价格不上涨，可成小幅回落，不会形成价格暴跌，因为已发行的 BTL 的存量的数量是确定的，有限的。而科学的发行方式，让 BTL 的每一个共识者、布道者、信仰者形成可遇见、可确定的 BTL 价格价值思维逻辑。逢 BTL 价格小幅回落时，会对已知 BTL 存量形成强大的买入。

BTL 是整个 BTLink 公链所有商业生态的唯一通证，钱包每次转账必须支付 BTL 通证作为公链的使用费用。因此每一个运行在 BTLink 的项目方，逢存量的 BTL 价格小幅回落时，会形成大量买入。首先自身项目内容要使用 BTL，公链转账要支付 BTL。在 BTLink 发布项目的项目方，发布建立项目也是为了创造经济利益，因此 BTLink 上的项目方会长期持有 BTL，逢 BTL 价格回落时正式买入 BTL 的时机。

因此，BTLink 公链 BTL 通证的发行算法，完全符合市场经济，更加科学，更加伟大。科学严谨的发行算法，能让 BTL 通证可以快速的达成共识，不在像比特币等公链的数字资产，走过 13 年漫长的发展，币价经过数次 90%，很多次 50%以上的跌幅。而这种科学的发行方式，可能会改变现有世界金融，有牛熊市的周期。在 BTL 形成共识初级阶段，形成慢牛;在不断形成的慢牛的过程中，这种稳健的财富获得方式，最终会传导全世界，让 BTL 形成长期牛市。不管机构、财团、经济体和全世界的人们都一样，买涨不买跌。即使投资大师股神:沃伦•巴菲特，一直倡导价值投资，复利是可创造财富奇迹。沃伦•巴菲特的投资名言:“别人贪婪的时候要恐慌，别人恐慌的时候要贪婪”，其实巴菲特深知经济有牛熊周期，因此一定要在价

值投资的标的物上，下跌和暴跌的时候买入，然后耐心的等待上涨。其实巴菲特对价值标的物逢暴跌买入，以更低价格买入，是为了降低买入的投资风险，因为巴菲特也不能保证自己买入的股票百分之百的上涨。巴菲特一生都在坚持和倡导价值投资，因为价值投资风险相对较小，而当价值股票暴跌逢低买入，首先降低投资风险，减少买入成本，从而在牛市迎来更多上涨。因此投资大师沃伦•巴菲特也和普通人一样，依然是“买涨不买跌”。

因此，BTLink 完全符合市场经济学的科学发行算法，可遇见、可确定，可期待，可让投资者建立价值投资思维、最后形成行为投资逻辑。充分保障了每一个共识者、布道者、信仰者、囤币者的核心利益。让 BTL 通证价格呈涌动式、螺旋式的上涨。web2.0 让互联网创造万亿商机，让无数平民创业者成为了财富的主人，融入了世界经济。而 web3.0，去中心化的区块链互联网，将颠覆 web2.0，创造兆亿财富。世界的下 100 年至 1000 年，人类都将生活在更为广阔的互联网时代。

如果您错过了 2009 年的比特币:Bitcoin，请遇见今天更加美好的 BTLink:BTL。

目录

杂项和关注

改进版幽灵协议的实施

费用

计算和图灵完备

货币和发行

BTL 市值发行机制如下

关于 BTLink 的分解

BTLink 区块链商城

BTLink 公链区块链加密存储

虚拟生态场景

BTLink 区块链游戏生态

BTLink 去中心化交易所

BTLink 加密社交金融

BTLink 跨链

综述：去中心化应用

发展背景

去中心化的数字货币概念，正如财产登记这样的替代应用一样，早在几十年以前就被提出来了。1980 和 1990 年代的匿名电子现金协议，大部分是以乔姆盲签技术（Chaumian blinding）为基础的。这些电子现金协议提供具有高度隐私性的货币，但是这些协议都没有流行起来，因为它们都依赖于一个中心化的中介机构。1998 年，戴伟（Wei Dai）的 b-money 首次引入了通过解决计算难题和去中心化共识创造货币的思想，但是该建议并未给出如何实现去中心化共识的具体方法。2005 年，芬尼（Hal Finney）引入了“可重复使用的工作量证明机制”（reusable proofs of work）概念，它同时使用 b-money 的思想和 Adam Back 提出的计算困难的哈希现金（Hashcash）难题来创造密码学货币。但是，这种概念再次迷失于理想化，因为它依赖于可信任的计算作为后端。

因为货币是一个先申请应用，交易的顺序至关重要，所以去中心化的货币，需要找到实现去中心化共识的方法。比特币以前的所有电子货币协议，所遇到的主要障碍是，尽管对如何创建安全的拜占庭问题，容错（Byzantine-fault-tolerant）多方共识系统的研究已经历时多年，但是上述协议只解决了问题的一半。这些协议假设系统的所有参与者是已知的，并产生如“如果有 N 方参与到系统中，那么系统可以容忍 N/4 的恶意参与者”这样形式的安全边界。然而这个假设的问题在于，在匿名的情况下，系统设置的安全边界容易遭受女巫攻击，因为一个攻击者，可以在一台服务器，或者僵尸网络上创建数以千计的节点，从而单方面确保拥有多数份额。

中本聪的创新是引入这样一个理念：将一个非常简单的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。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。拥有大量算力的节点有更大的影响力，但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。尽管比特币区块链模型非常简单，但是实践证明它已经足够好用了，在未来五年到30年，它将成为全世界两百个以上经济体的货币锚定物（如黄金）和协议的基石。

中本聪在2009年1月3日，在比特币创世区块上写下：“英国的财务大臣又开始第二轮货币援助，这种无限印刷钞票的信用货币体系，造成世界通货膨胀，让各种生活物资和各种生产资料不断涨价，货币贬值得像纸一样，让世界底层人民永远生活在高通胀的世界。而比特币开源恒量2100万枚，每一笔交易，由交易者自我掌控私钥签名交易，无需中心化的交易授权，每笔交易由参与记账的节点全网广播确认。这是一个人类金融史、货币上一次伟大的实验和革命，货币和资产的发行、交易，由每一个使用的人们，自己发行自己的货币，通过私钥自己掌控自己货币和资产。每一个参与者，就是“比特币央行的行长”;每一笔比特币交易记账的节点，就是比特币的发行者。因此比特是世界人民的货币，它不属于任何中心化的经济体，公司、个人包括中本聪!

2009年中本聪创世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），一种去中心化的点对点的网上货币，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。到目前为止，比特币已经吸引了全世界人们注意力、国家、世界500强企业、保险巨头、银行、财团、家族办公室的认可以及参与。人类社会从web1.0，进入到web2.0，现在全面进入web3.0互联网时代;从1.0，2.0 的中心化互联网，全面进入到3.0去中心化的互联网时代! 黄金，这个贵金属，从古到今，不论王朝更迭，始终是人类社会的硬通货，可以兑换然后物质和商品，因为性能稳定，数量稀少，开采成本不断增高，黄金是钞票中的钞票。而比特币是人类下100-1000年，人类互联网时代的数字黄金，可以成为中心化经济体信仰货币的锚定物，也可以成为世界企业各种证券票据的托底物，更也可以和黄金兑换世界任何一种物质。比特币才13岁，犹如一个儿童，刚刚进入青年。下一个10年，是比特币、区块链成长的10年，应用的10年，落地的10年，更是全球立法的10年。就政治方面而言，它是一种没有中央银行的货币，是由参与挖矿的世界人民发行，因此比特币在全球有一个名牌称号“人民的货币”。黄金有五千年的共识，比特币仅13年的一个共识，而人类下1000年互联网的世界，比特币今天剧烈的价格波动将逐步减小，成为数字黄金。

然而，中本聪的伟大试验还有与比特币同等重要的一部分：基于工作量证明的区块链概念，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1BTC并且同时向A和B发送这1BTC，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，全世界开发者们的注意力开始迅速地转向比特币技术的第二部分，区块链怎样应用于货币以外的web3.0去中心化的区块链互联网领域。

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：

<code style="font-family:Menlo, Courier, monospace, monospace, sans-serif;font-size:13.6px;margin:0px;border:none;background-color:transparent;white-space:pre-wrap;" class="hljs">APPLY(S,TX)  > S’ or ERROR</code>

在上面提到的银行系统中，状态转换函数如下：

<code style="font-family:Menlo, Courier, monospace, monospace, sans-serif;font-size:13.6px;margin:0px;border:none;background-color:transparent;white-space:pre-wrap;" class="hljs">APPLY({ Alice: $50, Bob: $50 },” send $20 from Alice to Bob”) = { Alice: $30,Bob: $70 }</code>

但是：

<code style="font-family:Menlo, Courier, monospace, monospace, sans-serif;font-size:13.6px;margin:0px;border:none;background-color:transparent;white-space:pre-wrap;" class="hljs">APPLY({ Alice: $50, Bob: $50 },” send $70 from Alice to Bob”) = ERROR</code>

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[1]）。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：

1.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

2.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

3.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。

4.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。

挖矿

如果我们拥有可信任的中心化服务机构，状态转换系统可以很容易地实现，可以简单地将上述功能准确编码。然而，我们想把比特币系统，建成为去中心化的货币系统，为了确保每个人都同意交易的顺序，我们需要将状态转换系统与一个共识系统结合起来。比特币的去中心化，共识进程要求网络中的节点，不断尝试将交易打包成“区块”。网络被设计为大约每十分钟产生一个区块，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：

1.检查区块引用的上一个区块是否存在且有效。

2.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]。

3.检查区块的工作量证明是否有效。

4.将上一个区块的最终状态赋于 S[0]。

5.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。

6.返回正确，状态 S[n]是这一区块的最终状态。

7.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，包括作为比特币发明创造者中本聪也没有比特币。

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：

1.向卖家发送 1BTC 购买商品（尤其是无需邮寄的电子商品）。

2.等待直至商品发出。

3.创建另一笔交易，将相同的 1BTC 发送给自己的账户。

4.使比特币网络相信发送给自己账户的交易是最先发出的。

5.一旦步骤（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）。

默克尔树

左：仅提供默克尔树（Merkle tree）上的少量节点已经足够给出分支的合法证明。

右：任何对于默克尔树的任何部分进行改变的尝试都会最终导致链上某处的不一致。

比特币系统的一个重要的可扩展特性是：它的区块存储在多层次的数据结构中。一个区块的哈希实际上只是区块头的哈希，区块头是包含时间戳、随机数、上个区块哈希和存储了所有的区块交易的默克尔树的根哈希的长度大约为 200 字节的一段数据。

默克尔树是一种二叉树，由一组叶节点、一组中间节点和一个根节点构成。最下面的大量的叶节点包含基础数据，每个中间节点是它的两个子节点的哈希，根节点也是由它的两个子节点的哈希，代表了默克尔树的顶部。默克尔树的目的是允许区块的数据可以零散地传送：节点可以从一个源下载区块头，从另外的源下载与其有关的树的其它部分，而依然能够确认所有的数据都是正确的。之所以如此是因为哈希向上的扩散：如果一个恶意用户尝试在树的下部加入一个伪造的交易，所引起的改动将导致树的上层节点的改动，以及更上层节点的改动，最终导致根节点的改动以及区块哈希的改动，这样协议就会将其记录为一个完全不同的区块（几乎可以肯定是带着不正确的工作量证明的）。

默克尔树协议对比特币的长期持续性可以说是至关重要的。在 2014 年 4 月，比特币网络中的一个全节点-存储和处理所有区块的全部数据的节点-需要占用 15GB 的内存空间，而且还以每个月超过 1GB 的速度增长。目前，这一存储空间对台式计算机来说尚可接受，但是手机已经负载不了如此巨大的数据了。未来只有商业机构和爱好者才会充当完整节点。简化支付确认（SPV)协议允许另一种节点存在，这样的节点被成为“轻节点”，它下载区块头，使用区块头确认工作量证明，然后只下载与其交易相关的默克尔树“分支”。这使得轻节点只要下载整个区块链的一小部分，就可以安全地确定任何一笔比特币交易的状态和账户的当前余额。

其它的区块链应用

将区块链的思想应用到其它领域的想法早就出现了。在 2005 年，尼克萨博提出了“用所有权为财产冠名”的概念，文中描述了复制数据库技术的发展如何使基于区块链的系统可以应用于登记土地所有权，创建包括例如房产权、违法侵占和乔治亚州土地税等概念的详细框架。然而，不幸的是在那时还没有实用的复制数据库系统，所以这个协议被没有被付诸实践。不过，自 2009 年比特币系统的去中心化共识开发成功以来，许多区块链的其它应用开始快速出现。

域名币（namecoin）- 创建于 2010 年，被称为去中心化的名称注册数据库。像 Tor、Bitcoin 和 BitMessage 这样的去中心化协议，需要一些确认账户的方法，这样其他人才能够与用户进行交互。但是，在所有的现存的解决方案中仅有的可用的身份标识是象 1LW79wp5ZBqaHW1jL5TciBCrhQYtHagUWy 这样的伪随机哈希。理想的情况下，人们希望拥有一个带有象“george”这样的名称的账户。然而，问题是如果有人可以创建“george”账户，那么其他人同样也可以创建“george”账户来假扮。唯一的解决方法是先申请原则（first-to-file），只有第一个注册者可以成功注册，第二个不能再次注册同一个账户。这一问题就可以利用比特币的共识协议。域名币是利用区块链实现名称注册系统的最早的、最成功的系统。

彩色币（Colored coins）- 彩色币的目的是为人们在比特币区块链上创建自己的数字货币，或者，在更重要的一般意义上的货币 - 数字令牌提供服务。依照彩色币协议，人们可以通过为某一特别的比特币 UTXO 指定颜色，发行新的货币。该协议递归地将其它 UTXO 定义为与交易输入 UTXO 相同的颜色。这就允许用户保持只包含某一特定颜色的 UTXO，发送这些 UTXO 就像发送普通的比特币一样，通过回溯全部的区块链判断收到的 UTXO 颜色。

元币（Metacoins）- 元币的理念是在比特币区块链上创建新的协议，利用比特币的交易保存元币的交易，但是采用了不同的状态转换函数 APPLY’。因为元币协议不能阻止比特币区块链上的无效的元币交易，所以增加一个规则如果 APPLY’(S,TX)返回错误，这一协议将默认 APPLY’(S,TX) = S。这为创建任意

的、先进的不能在比特币系统中实现的密码学货币协议提供了一个简单的解决方法，而且开发成本非常低，因为挖矿和网络的问题已经由比特币协议处理好了。

因此，一般而言，建立共识协议有两种方法：建立一个独立的网络和在比特币网络上建立协议。虽然像域名币这样的应用使用第一种方法已经获得了成功，但是该方法的实施非常困难，因为每一个应用需要创建独立的区块链和建立、测试所有状态转换和网络代码。另外，我们预测去中心化共识技术的应用将会服从幂律分布，大多数的应用太小不足以保证自由区块链的安全，我们还注意到大量的去中心化应用，尤其是去中心化自治组织，需要进行应用之间的交互。

另一方面，基于比特币的方法存在缺点，它没有继承比特币可以进行简化确认支付（SPV）的特性。比特币可以实现简化确认支付，因为比特币可以将区块链深度作为有效性确认代理。在某一点上，一旦一笔交易的祖先们距离现在足够远时，就可以认为它们是合法状态的一部分。与之相反，基于比特币区块链的元币协议不能强迫区块链不包括不符合元币协议的交易。因此，安全的元币协议的简化支付确认需要后向扫描所有的区块，直到区块链的初始点，以确认某一交易是否有效。目前，所有基于比特币的元币协议的“轻”实施都依赖可信任的服务器提供数据，这对主要目的之一是消除信任需要的密码学货币而言，只是一个相当次优的结果。

脚本

即使不对比特币协议进行扩展，它也能在一定程度上实现”智能合约”。比特币的 UTXO 可以被不只一个公钥拥有，也可以被用基于堆栈的编程语言所编写的更加复杂的脚本所拥有。在这一模式下，花费这样的 UTXO，必须提供满足脚本的数据。事实上，基本的公钥所有权机制也是通过脚本实现的：脚本将椭圆曲线签名作为输入，验证交易和拥有这一 UTXO 的地址，如果验证成功，返回 1，否则返回 0。更加复杂的脚本用于其它不同的应用情况。例如，人们可以创建要求集齐三把私钥中的两把才能进行交易确认的脚本（多重签名），对公司账户、储蓄账户和某些商业代理来说，这种脚本是非常有用的。脚本也能用来对解决计算问题的用户发送奖励。人们甚至可以创建这样的脚本“如果你能够提供你已经发送一定数额的的狗币给我的简化确认支付证明，这一比特币 UTXO 就是你的了”，本质上，比特币系统允许不同的密码学货币进行去中心化的兑换。

然而，比特币系统的脚本语言存在一些的限制：

缺少图灵完备性 - 这就是说，尽管比特币脚本语言可以支持多种计算，但是它不能支持所有的计算。最主要的缺失是循环语句。不支持循环语句的目的是避免交易确认时出现无限循环。理论上，对于脚本程序员来说，这是可以克服的障碍，因为任何循环都可以用多次重复 if 语句的方式来模拟，但是这样做会导致脚本空间利用上的低效率，例如，实施一个替代的椭圆曲线签名算法可能将需要 256 次重复的乘法，而每次都需要单独编码。

价值盲（Value-blindness）。UTXO 脚本不能为账户的取款额度提供精细的控制。例如，预言机合约（oracle contract）的一个强大应用是对冲合约，A 和 B 各自向对冲合约中发送价值 1000 美元的比特币，30 天以后，脚本向 A 发送价值 1000 美元的比特币，向 B 发送剩余的比特币。虽然实现对冲合约需要一个预言 机（oracle）决定一比特币值多少美元，但是与现在完全中心化的解决方案相比，这一机制已经

在减少信任和基础设施方面有了巨大的进步。然而，因为 UTXO 是不可分割的，为实现此合约，唯一的方法是非常低效地采用许多有不同面值的 UTXO（例如对应于最大为 30 的每个 k，有一个 2^k 的 UTXO)并使预言机挑出正确的 UTXO 发送给 A 和 B。

缺少状态 - UTXO 只能是已花费或者未花费状态，这就没有给需要任何其它内部状态的多阶段合约或者脚本留出生存空间。这使得实现多阶段期权合约、去中心化的交换要约或者两阶段加密承诺协议（对确保计算奖励非常必要）非常困难。这也意味着 UTXO 只能用于建立简单的、一次性的合约，而不是例如去中心化组织这样的有着更加复杂的状态的合约，使得元协议难以实现。二元状态与价值盲结合在一起意味着另一个重要的应用-取款限额-是不可能实现的。

区块链盲（Blockchain-blindness）- UTXO 看不到区块链的数据，例如随机数和上一个区块的哈希。这一缺陷剥夺了脚本语言所拥有的基于随机性的潜在价值，严重地限制了博彩等其它领域应用。

我们已经考察了在密码学货币上

POW 机制的优缺点如下：

优点:

1.POW 机制本身是很复杂的，在这其中有很多细节。例如：挖矿难度自动调整、区块奖励逐渐减半等，这些因素都是根据经济学原理，能够吸引和激励更多人参与。

2.理想状态。POW 机制可以引来很多用户参加，尤其是越先参与的得到越多，这样会促使加密货币的初始阶段发展非常迅速，节点网络的迅速扩大。在 Cpu 挖矿的时代，比特币就吸引了非常多的人参与“挖矿”，这就是很好的证明。

3.通过“挖矿”的方式进行新币发行，把比特币散发给个人，实现了相对公平。

缺点：

1.算力是计算机硬件（Cpu、Gpu 等）提供的，需要消耗电力，是对能源的直接消耗，违背人类追求节能、清洁、环保的理念。

2.POW 机制发展到现在，算力的提供已经不是单纯的 CPU 了，已经是逐步发展到 GPU、FPGA，甚至是 ASIC 矿机。用户也从原本的个人挖矿发展到现在的大的矿池、矿场，算力集中越来越明显。这与去中心化的方向完全相反，网络的安全也在慢慢受到威胁。有证据证明 Ghash（一个矿池）就曾经对赌博网站实行了双花攻击（意思就是一笔钱花两次）。

3.比特币区块奖励每 4 年就会减半，当挖矿的成本超过挖矿收益时，用户挖矿的积极性肯定就会降低，会有大量算力减少，比特币网络的安全性将进一步堪忧。

BTLinkDPoS 的诞生

DPoS (Delegated Proof of Stake) 股份权益证明机制,是人类区块链发展史上趋势性的共识算法。2014 年 4 月由 Bitshares 的首席开发者 Dan Larimer 提出并应用。当时 Dan 观察到比特币系统共识算法 POW 的一些问题：比如矿池导致算力越来越集中、电力耗费过大等。所以他提出了一种更加快速、安全且能源消耗比较小的算法，这就是后来的 DPOS。BTLinkDPOS 是所有股东算力节点的共识算法，由全球股东算力节点共同来治理和运营公链网络。BTLinkDPOS 机制中，不需要算力解决数学难题，而是由全球所有 BTLink 的股东算力节点治理和运行公链网络，这也就解决了 POS、Dpos 的公平、公正、公开和安全性能问题，真正实现人人共同参与，共同治理。BTLink 全球初始发行 42000 个股东算力节点，节点社区分别通过个钱包地址获取 BTLink 通证。42000 个股东算力节点参与全网全球第一批节点挖矿分红。每次 BTL 市值上涨将把剩余的所有 BTL 通证，发行给全球的股东算力节点，其价值与不亚于比特币和以太坊的价值。

BTlinkDPoS 的运作机制

1. 所有股东算力节点共同保障 BTLink 公链的正常运行；

2. 收集网络里的交易；

3. 股东算力节点验证交易，把交易打包到区块；

4. 股东算力节点广播区块，其他算力节点验证后把区块添加到自己的数据库；

5. 股东算力节点带领并促进 BTLink 区块链项目的发展。

所有股东算力节点相当于比特币网络里的矿机，在完成本职工作的同时，可以获得 BTLink 全网所有剩余 BTL 的发行奖励，和比特币的矿工一下，可以获得比特币全网 BTC 的挖矿奖励。

在 BTlinkDPOS 机制下，算法要求系统做三件事：

第一，随机指定生产者出场顺序；

第二，不按顺序生产的区块无效；

第三，每过一个周期洗牌一次，打乱原有顺序；

**BTlinkDPOS 机制涉及如下几个问题：**

1. 股东算力节点持有 BTL

直接在交易平台上购买相应数量 BTL，到 BTLink 公链进行质押获得权益后，即可获得股东算力节点相应权益。

2. 成为算力节点

成为 BTLink 的股东算力节点，你必须在网络上注册你的公钥，分配到一个 32 位的特有标识符，该标识符会被每笔交易数据的“头部”引用。

3. 保持股东算力节点，获得剩余 BTL 通证余量发行

每个钱包将显示一个状态指示器，让用户知道他们的股东节算力点表现怎么样。每一个 BTLink 的股东算力节点，公链上线时将相应数量 BTL 记录表达写入 BTLink 的公链算法里，就可以获得所有 BTL 余量的发行。

4. 抵抗攻击

在抵抗攻击上，因为42000股东算力节点所获得的权力权是相同的，每名股东算力节点都有一份一比一相等的投票权。并且，如果当前记账节点不记账，则由下一个股东记账人记账。

因为有42000个股东算力节点，可以想象一个攻击者，很难对每名轮生产区块的股东算力节点，依次进行拒绝服务攻击。

而且，由于事实上每一个股东算力节点的标识是其公钥而非IP地址，使得确定拒绝服务攻击目标更为困难，这种特定攻击的威胁很容易被减轻。

**BTlinkDPOS机制遵从如下几条基本原则：**

1. 持有通证的股东算力 节点，依据所持BTL的钱包地址行使表决权，而不是依赖挖矿竞争记账权。

2. 最大化持有的盈利。

3. 最小化维护网络安全的费用。

4. 最大化网络的效能。

5. 最小化运行网络的成本（带宽、CPU等）。

BTLink账户

BTLink公链将是web3.0去中心化区块链互联网，宇宙和地球上最早期的去中心化区块链互联网协议，也将在宇宙星际间和地球上，成为运用范围最广泛的去中心化区块链互联网协议。其基本功能组成包括共识机制：DPos或BlockDAG（此处根据具体开发情况来决定共识），智能合约支持，支持Web3，支持智能合约集成EVM（非WASM）；需要使用隐私加密算法（由技术方基于当前技术开发进行决定）等等。

目前，全球上千万个区块链项目，都是在Etherscan、TRONscan、BSCscan区块链创建、运行。BTLink公链通过创建一个对开发者友好的区块链底层平台，支持允许任何人在平台中建立应用，和使用通过区块链技术运行的去中心化应用，允许用户按照自己的意愿创建复杂的操作，HEYTF区块链系统定制开发，
BTLink公链开153发7537等7737服务项目，经验丰富。

（1）保护用户权益免受程序开发者的影响

在BTLink公链中程序的开发者没有权利干涉用户，所以BTLink公链可以保护使用该程序的用户权益。此外，高度去中心化的分布式数据存储也是BTLink公链最大的特点之一，交易数据公开透明化、数据无法篡改等优点，使BTLink公链可以有效保障用户的数据安全。

（2）产生网络效应

一种信息产品存在着互联的内在需要，因为人们生产和使用它们的目的，就是更好地收集和交流信息。随着网络规模的扩大，用户能从中获取更多的价值，需求得到更大的满足。BTLink 公链具有开放性，因此有机会，被很多的外界用户应用，并逐步广泛产生巨大程度的网络效应。

（3）落地应用于实际商业场景

任何对信任、安全和持久性要求较高的应用场景，比如资产注册、投票、管理和物联网等 web3.0 时代的应用，都会大规模地受到 BTLink 公链的影响和渗透、参与和和互动。

BTLink 技术团队，通过无数次的实验、验证，获得领先全球的商业应用技术，可以在卡、卷、杯、盒等所有外包装上印制镶嵌含 BTL 钱包地址的二维码，可在全球范围内实现大规模的商业应用，让消费者体验消费金融，体验 Web3.0 价值互联网;为商业企业创造更多持续稳定的消费者，更多消费应用场景，让商业触链，生意不难。减少无效的广告营销，缔造全球新商业、新消费、新金融。让商业和人类更加和谐，降低人类活动的碳排放，让地球家园更加绿色环保。

通过 VR、AR、XR，跨链、物联网等革命性的技术协议，完成万物互联互通，推动世界实现智能地球，智慧地球。

在 BTLink 系统中，状态是由被称为“账户”（每个账户由一个 20 字节的地址）的对象和在两个账户之间转移价值和信息的状态转换构成的。BTLink 的账户包含四个部分：

随机数，用于确定每笔交易只能被处理一次的计数器

账户目前的 BTLink 余额

账户的合约代码

账户的存储

BTL 是 BTLink 公链所有生态的主要加密燃料，用于支付交易费用。一般而言，BTLink 有两种类型的账户：外部所有的账户（由私钥控制的）和合约账户（由合约代码控制）。外部所有的账户没有代码，人们可以通过创建和签名一笔交易从一个外部账户发送消息。每当合约账户收到一条消息，合约内部的代码就会被激活，允许它对内部存储进行读取和写入，和发送其它消息或者创建合约。

代码执行

BTLink 合约的代码使用高级的基于堆栈的字节码的语言写成的，被称为“BTLink 虚拟机代码”。代码由一系列字节构成，每一个字节代表一种操作。一般而言，代码执行是无限循环，程序计数器每增加一（初始值为零）就执行一次操作，直到代码执行完毕或者遇到错误，STOP 或者 RETURN 指令。操作可以访问三种存储数据的空间：

堆栈，一种后进先出的数据存储，32 字节的数值可以入栈，出栈。

内存，可无限扩展的字节队列。
合约的长期存储，一个秘钥/数值的存储，其中秘钥和数值都是 32 字节大小，与计算结束即重置的堆栈和内存不同，存储内容将长期保持。

代码可以象访问区块头数据一样访问数值，发送者和接受到的消息中的数据，代码还可以返回数据的字节队列作为输出。

当 BTLink 虚拟机运行时，它的完整的计算状态可以由元组(block_state, transaction, message, code, memory, stack, pc, gas)来定义，这里 block_state 是包含所有账户余额和存储的全局状态。每轮执行时，通过调出代码的第 pc（程序计数器）个字节，当前指令被找到，每个指令都有定义自己如何影响元组。例如，ADD 将两个元素出栈并将它们的和入栈，每笔 GAS 以金本位计算，GAS 费用全球最低。为繁荣全球 Web3.0，代码算法，自动智能调节，可执行“零”GAS。这种 GAS 智能算法，将开创和引领 Web3.0 向前发展，充分友好应用的创建者，和应用的使用者。

这几年不来了 SSTORE 将顶部的两个元素出栈并将第二个元素插入到由第一个元素定义的合约存储位置，虽然有许多方法通过即时编译去优化 BTLink，但 BTLink 的基础性的实施可以用几百行代码实现。

区块链和挖矿

虽然有一些不同，但 BTLink 的区块链在很多方面类似于比特币区块链。它们的区块链架构的不同在于，BTLink 区块不仅包含交易记录和最近的状态，还包含区块序号和难度值。BTLink 中的区块确认算法如下：

1. 检查区块引用的上一个区块是否存在和有效。
2. 检查区块的时间戳是否比引用的上一个区块大，而且小于 1 分钟。
3. 检查区块序号、难度值、 交易根，叔根和燃料限额（许多 BTLink 特有的底层概念）是否有效。
4. 检查区块的 Dpos 权益工作量证明是否有效。
5. 将 S[0]赋值为上一个区块的 STATE_ROOT。
6. 将 TX 赋值为区块的交易列表，一共有 n 笔交易。对于属于 0……n-1 的 i，进行状态转换 S[i+1] = APPLY(S[i],TX[i])。如果任何一个转换发生错误，或者程序执行到此处所花费的燃料（gas）超过了 GASLIMIT，返回错误。
7. 用 S[n]给 S_FINAL 赋值，向 Dpos 权益证明的矿工支付区块奖励。
8. 检查 S-FINAL 是否与 STATE_ROOT 相同。如果相同，区块是有效的。否则，区块是无效的。

BTLink 以格林威治时间，1 秒为单位进行每个区块爆块，到账时间一般 1 秒单位到账，远远高于比特币和其他公链。原因是状态存储在树结构中（tree structure），每增加一个区块，只需要改变树结构的一小部分。因此，一般而言，两个相邻的区块的树结构的大部分应该是相同的，因此存储一次数据，可以利用指针（即子树哈希）引用两次。一种被称为“帕特里夏树”（“Patricia Tree”）的树结构可以实现这一点，其中包括了对默克尔树概念的修改，不仅允许改变节点，而且还可以插入和删除节点。另外，因为

所有的状态信息是最后一个区块的一部分，所以没有必要存储全部的区块历史-这一方法如果能够可以应用到比特币系统中，经计算可以对存储空间有 10-20 倍的节省。

应用

BTLink 之上有三种应用。第一类是金融应用，为用户提供更强大的用他们的钱包管理和参与合约的方法。包括子货币，金融衍生品，对冲合约，储蓄钱包，商业合同、财务系统、基金保险、信托、遗嘱，甚至一些种类的全面的雇佣合约。第二类是半金融应用，这里有钱的存在但也有很重的非金钱的方面，一个完美的例子是为解决计算问题，而设的自我强制悬赏。最后，还有在线投票和去中心化治理这样的完全的非金融应用。

令牌系统

链上令牌系统有很多应用，从代表如美元或黄金等资产的子货币到公司股票，单独的令牌代表智能资产，安全的不可伪造的优惠券，甚至与传统价值完全没有联系的用来进行积分奖励的令牌系统。在 BTLink 中实施令牌系统容易得让人吃惊。关键的一点是理解，所有的货币或者令牌系统，从根本上来说是一个带有如下操作的数据库：从 A 中减去 X 单位并把 X 单位加到 B 上，前提条件是(1)A 在交易之前有至少 X 单位以及(2)交易被 A 批准。实施一个令牌系统，就是把这样一个逻辑实施到一个合约中去。

用 Serpent 语言实施一个令牌系统的基本代码如下：

```
<code style="font-family:Menlo, Courier, monospace, monospace, sans-serif;font-size:13.6px;margin:0px;border:none;background-color:transparent;white-space:pre-wrap;" class="hljs">from = msg.sender

to = msg.data[0]


value = msg.data[1]

if contract.storage[from] >= value:


contract.storage[from] = contract.storage[from] value


contract.storage[to] = contract.storage[to] + value</code>
```

BTLink 将要进一步描述的“银行系统”状态转变功能的一个最小化实施。需要增加一些额外的代码以提供在初始，和其它一些边缘情况下分发货币的功能。理想情况下，会增加一个函数，让其它合约来查询一个地址的余额，就足够了。理论上，基于 BTLink 的充当子货币的令牌系统，可能包括一个基于比特币的

链上元币所缺乏的重要功能：直接用这种货币支付交易费的能力。实现这种能力的方法是在合约里，维护一个 BTLink 账户以用来为发送者支付交易费，通过收集被用来充当交易费用的内部货币，并把它们在一个不断运行的拍卖中拍卖掉，合约不断为该 BTLink 账户注资。这样用户需要用 BTL“激活”他们的账户，一旦账户中有 BTL，它将会被重复使用因为每次合约都会为其充值。

金融衍生品和价值稳定的货币

金融衍生品是“智能合约”的最普遍的应用，也是最易于用代码实现的之一。实现金融合约的主要挑战，是它们中的大部分，需要参照一个外部的价格发布器；例如，一个需求非常大的应用，是一个用来对冲 BTL（或其它密码学货币），相对美元价格波动的智能合约，但该合约需要知道 BTL 相对美元的价格。最简单的方法是通过由某特定机构（例如纳斯达克）维护的“数据提供“合约进行，该合约的设计使得该机构能够根据需要更新合约，并提供一个接口，使得其它合约能够通过，发送一个消息给该合约，以获取包含价格信息的回复。

当这些关键要素都齐备，对冲合约看起来会是下面的样子：

等待 A 输入 1OBTL。

等待 B 输入 1OBTL。

通过查询数据提供合约，将 1OBTL 的美元价值，例如，x 美元，记录至存储器。

30 天后，允许 A 或 B“重新激活“合约以发送价值 x 美元的 BTL（重新查询数据提供合约，以获取新价格并计算）给 A 并将剩余的 BTL 发送给 B。

这样的合约在密码学商务中有非同寻常的潜力。密码学货币，经常被诟病的一个问题就是其价格的波动性；虽然大量的用户和商家，可能需要密码学资产所带来的安全和便利，可他们不太会乐意面对，一天中资产跌去百分之二三十价值的情形。直到现在，最为常见的推荐方案是发行者背书资产；思想是发行者创建一种子货币，对此种子货币他们有权发行和赎回，给予（线下）提供给他们一个单位特定相关资产（例如黄金，美元）的人一个单位子货币。发行者承诺当任何人送还一个单位密码学资产时。发还一个单位的相关资产。这种机制能够使任何非密码学资产被“升级“为密码学资产，如果发行者值得信任的话。

然而实践中发行者并非总是值得信任的，并且一些情况下银行体系太脆弱，或者不够诚实守信从而使这样的服务无法存在。金融衍生品提供了一种替代方案。这里将不再有提供储备，以支撑一种资产的单独的发行者，取而代之的是一个，由赌一种密码学资产的价格会上升的投机者构成的去中心化市场。与发行者不同，投机者一方没有讨价还价的权利，因为对冲合约把他们的储备冻结在了契约中。注意这种方法并非是完全去中心化的，因为依然需要一个可信任的提供价格信息的数据源，尽管依然有争议这依然是在降低基础设施需求（与发行者不同，一个价格发布器不需要牌照并且似乎可归为自由言论一类），和降低潜在欺诈风险方面的一个伟大的进步。

身份和信誉系统

最早的替代币，域名币，尝试使用一个类比特币块链，来提供一个名称注册系统，在那里用户，可以将他们的名称，和其它数据一起在一个公共数据库注册。最常用的应用案例把象“bitcoin.org“（或者再域名币中，”bitcoin.bit“）一样的域名与一个 IP 地址对应的域名系统。其它的应用案例包括电子邮件验证系统，和潜在的更先进的信誉系统。这里是 BTLink 中提供与域名币类似的的名称注册系统的基础合约：

<code style="font-family:Menlo, Courier, monospace, monospace, sans-serif;font-size:13.6px;margin:0px;border:none;background-color:transparent;white-space:pre-wrap;" class="hljs">if !contract.storage[tx.data[0]]:

contract.storage[tx.data[0]] = tx.data[1]</code>

合约非常简单；就是一个 BTLink 网络中的可以被添加，但不能被修改或移除的数据库。任何人都可以把一个名称注册为一个值并永远不变。一个更复杂的名称注册合约，将包含允许其他合约查询的“功能条款“，以及一个让一个名称的”拥有者“（即第一个注册者）修改数据或者转让所有权的机制。甚至可以在其上添加信誉和信任网络功能。

去中心化存储

在过去的几年里出现了一些链上分布式文件存储公司，Dropbox，它寻求允许用户上传他们的硬盘备份，提供备份存储服务并允许用户访问从而按月向用户收取费用。然而，在这一点上这个文件存储市场有时相对低效；对现存服务的粗略观察表明，特别地在“神秘谷“20-200GB 这一既没有免费空间也没有企业级用户折扣的水平上，主流文件存储成本，每月的价格意味着支付在一个月里，支付整个硬盘的成本。BTLink 合约允许去中心化存储生态的开发，这样用户通过将他们自己的硬盘，或未用的网络空间租出去以获得少量收益，从而降低了文件存储的成本。

这样的设施的基础性构件就是我们所谓的“去中心化 Dropbox 合约“。这个合约工作原理如下。首先，某人将需要上传的数据分成块，对每一块数据加密以保护隐私，并且以此构建一个默克尔树。然后创建一个含以下规则的合约，每 N 个块，合约将从默克尔树中抽取一个随机索引（使用能够被合约代码访问的上一个块的哈希来提供随机性）， 然后给第一个实体 BTLink 支撑一个带有类似简化验证支付（SPV）的在树中特定索引处的块的所有权证明。当一个用户想重新下载他的文件，他可以使用微支付通道协议（例如每 32k 字节支付 1 萨博）恢复文件；从费用上讲最高效的方法是支付者不到最后不发布交易，而是用一个略微更合算的带有同样随机数的交易在每 32k 字节之后来代替原交易。

这个协议的一个重要特征是，虽然看起来象是一个人信任许多不准备丢失文件的随机节点，但是他可以通过秘密分享把文件分成许多小块，然后通过监视合同得知每个小块都还被某个节点的保存着。如果一个合约依然在付款，那么就提供了某个人依然在保存文件的证据。

去中心化自治组织（DAO）

通常意义上“去中心化自治组织（DAO, decentralized autonomous organization）”的概念指的是一个拥有一定数量成员或股东的虚拟实体，依靠比如 67%多数来决定花钱以及修改代码。成员会集体决定组织

如何分配资金。分配资金的方法可能是悬赏，工资或者更有吸引力的机制比如用内部货币奖励工作。这仅仅使用密码学块链技术，就从根本上复制了传统公司，或者非营利组织的法律意义以实现强制执行。至此许多围绕DAO的讨论，都是围绕一个带有接受分红的股东，和可交易的股份的“去中心化自治公司（DAC，decentralized autonomous corporation）”的“资本家”模式；作为替代者，一个被描述为“去中心化自治社区（decentralized autonomous community）”的实体将使所有成员都在决策上拥有同等的权利并且在增减成员时要求67%多数同意。每个人都只能拥有一个成员资格这一规则需要被群体强制实施。

下面是一个如何用代码实现DO的纲要。最简单的设计就是一段如果三分之二成员同意，就可以自我修改的代码。虽然理论上代码是不可更改的，然而通过把代码主干放在一个单独的合约内并且把合约调用的地址指向一个可更改的存储依然可以容易地绕开障碍而使代码变得可修改，在一个这样的DAO合约的简单实现中有三种交易类型，由交易提供的数据区分：

[0,i,K,V] 注册索引为 i 的对存储地址索引为K 至 v 的内容的更改建议。
[0,i] 注册对建议 i 的投票。
[2,i] 如有足够投票则确认建议 i。

然后合约对每一项都有具体的条款。它将维护一个所有开放存储的更改记录以及一个谁投票表决的表。还有一个所有成员的表。当任何存储内容的更改获得了三分之二多数同意，一个最终的交易将执行这项更改。一个更加复杂的框架会增加内置的选举功能以实现如发送交易，增减成员，甚至提供委任制民主一类的投票代表（即任何人都可以委托另外一个人来代表自己投票，而且这种委托关系是可以传递的，所以如果A委托了B然后B委托了C那么C将决定A的投票）。这种设计将使DAO作为一个去中心化社区有机地成长，使人们最终能够把挑选合适人选的任务交给专家，与当前系统不同，随着社区成员不断改变他们的站队假以时日专家会容易地出现和消失。

一个替代的模式是去中心化公司，那里任何账户可以拥有0到更多的股份，决策需要三分之二多数的股份同意。一个完整的框架将包括资产管理功能-可以提交买卖股份的订单以及接受这种订单的功能（前提是合约里有订单匹配机制）。代表依然以委任制民主的方式存在，产生了“董事会”的概念。

更先进的组织治理机制可能会在将来实现；现在一个去中心化组织（DO）可以从去中心化自治组织（DAO）开始描述。DO和DAO的区别是模糊的，一个大致的分割线是治理是否可以通过一个类似政治的过程或者一个“自动”过程实现，一个不错的直觉测试是“无通用语言”标准：如果两个成员不说同样的语言组织还能正常运行吗？显然，一个简单的传统的持股式公司会失败，而像比特币协议这样的却很可能成功，罗宾·汉森的“futarchy”，一个通过预测市场实现组织化治理的机制是一个真正的说明“自治”式治理可能是什么样子的好例子。注意一个人无需假设所有DAO比所有DO优越；自治只是一个在一些特定场景下有很大优势的，但在其它地方未必可行的范式，许多半DAO可能存在。

进一步的应用 1. 储蓄钱包。 假设Alice想确保她的资金安全，但她担心丢失或者被黑客盗走私钥。她把BTL放到和Bob签订的一个合约里，如下所示，这合同是一个银行： ``` Alice单独每天最多可提取1%的资金。 Bob单独每天最多可提取1%的资金，但Alice可以用她的私钥创建一个交易取消Bob的提现权限。 Alice 和 Bob 一起可以任意提取资金。 一般来讲，每天1%对Alice足够了，如果Alice想提现更多她可以联系Bob寻求帮助。如果Alice的私钥被盗，她可以立即找到Bob把她的资金转移到一个新合

同里。如果她弄丢了她的私钥，Bob 可以慢慢地把钱提出。如果 Bob 表现出了恶意，她可以关掉他的提现权限。 ``` 2. 作物保险。一个人可以很容易地以天气情况而不是任何价格指数作为数据输入来创建一个金融衍生品合约。如果一个纽约的农民购买了一个基于纽约的降雨情况进行反向赔付的金融衍生品，那么如果遇到干旱，该农民将自动地收到赔付资金而如果有足量的降雨他会很开心因为他的作物收成会很好。3. 一个去中心化的数据发布器。 对于基于差异的金融合约，事实上通过过“谢林点”协议将数据发布器去中心化是可能的。谢林点的工作原理如下：N 方为某个指定的数据提供输入值到系统（例如 BTL/USDT 价格），所有的值被排序，每个提供 25%到 75%之间的值的节点都会获得奖励，每个人都有激励去提供他人将提供的答案，大量玩家可以真正同意的答案明显默认就是正确答案，这构造了一个可以在理论上提供很多数值，包括 BTL/USDT 价格，柏林的温度甚至某个特别困难的计算的结果的去中心化协议。 4. 多重签名智能契约。比特币允许基于多重签名的交易合约，例如，5 把私钥里集齐 3 把就可以使用资金。BTL 可以做得更细化，例如，5 把私钥里集齐 4 把可以花全部资金，如果只 3 把则每天最多花 10%的资金，只有 2 把就只能每天花 0.5%的资金。另外，BTL 里的多重签名是异步的，意思是说，双方可以在不同时间在区块链上注册签名，最后一个签名到位后就会自动发送交易。 5. 云计算。EVM 技术还可被用来创建一个可验证的计算环境，允许用户邀请他人进行计算然后选择性地要求提供在一定的随机选择的检查点上计算被正确完成的证据。这使得创建一个任何用户都可以用他们的台式机，笔记本电脑或者专用服务器参与的云计算市场成为可能，现场检查和安全保证金可以被用来确保系统是值得信任的（即没有节点可以因欺骗获利）。虽然这样一个系统可能并不适用所有任务；例如，需要高级进程间通信的任务就不易在一个大的节点云上完成。然而一些其它的任务就很容易实现并行；SETI@home, folding@home 和基因算法这样的项目就很容易在这样的平台上进行。 6. 点对点博彩。任意数量的点对点博彩协议都可以搬到 BTLink 的区块链上，例如 Frank Stajano 和 Richard Clayton 的 Cyberdice。 最简单的博彩协议事实上是这样一个简单的合约，它用来赌下一个区块的哈稀值与猜测值之间的差额，据此可以创建更复杂的博彩协议，以实现近乎零费用和无欺骗的博彩服务。 7. 预测市场。 不管是有神谕还是有谢林币，预测市场都会很容易实现，带有谢林币的预测市场可能会被证明是第一个主流的作为去中心化组织管理协议的“ futarchy”应用。 8. 链上去中心化市场，以身份和信誉系统为基础。

杂项和关注

改进版幽灵协议的实施

“幽灵“协议（”Greedy Heaviest Observed Subtree” (GHOST) protocol）是由 Yonatan Sompolinsky 和 Aviv Zohar 在 2013 年 12 月引入的创新。幽灵协议提出的动机是当前快速确认的块链因为区块的高作废率而受到低安全性困扰；因为区块需要花一定时间（设为 t）扩散至全网，如果矿工 A 挖出了一个区块然后矿工 B 碰巧在 A 的区块扩散至 B 之前挖出了另外一个区块，矿工 B 的区块就会作废并且没有对网络安全作出贡献。此外，这里还有中心化问题：如果 A 是一个拥有全网 30%算力的矿池而 B 拥有 10%的算力，A 将面临 70%的时间都在产生作废区块的风险而 B 在 90%的时间里都在产生作废区块。因此，如果作废率高，A 将简单地因为更高的算力份额而更有效率，综合这两个因素，区块产生速度快的块链很可能导致一个矿池拥有实际上能够控制挖矿过程的算力份额。

正如 Sompolinsky 和 Zohar 所描述的，通过在计算哪条链“最长”的时候把废区块也包含进来，幽灵协议解决了降低网络安全性的第一个问题；这就是说，不仅一个区块的父区块和更早的祖先块，祖先块的作废的后代区块（以 BTLink 术语中称之为“叔区块”）也被加进来以计算哪一个区块拥有支持其的最大工作量证明。我们超越了 Sompolinsky 和 Zohar 所描述的协议以解决第二个问题 – 中心化倾向，BTL 付

给以“叔区块”身份为新块确认作出贡献的废区块 64.8%的奖励，把它们纳入计算的“侄子区块”将获得奖励的 16.2%，不过，交易费用不奖励给叔区块。

BTLink 实施了一个只下探到第五层的简化版本的幽灵协议。其特点是，废区块只能以叔区块的身份被其父母的第二代至第五代后辈区块，而不是更远关系的后辈区块（例如父母区块的第六代后辈区块，或祖父区块的第三代后辈区块）纳入计算。这样做有几个原因。首先，无条件的幽灵协议将给计算给定区块的哪一个叔区块合法带来过多的复杂性。其次，带有 BTLink 所使用的补偿的无条件的幽灵协议剥夺了矿工在主链而不是一个公开攻击者的链上挖矿的激励。最后，计算表明带有激励的五层幽灵协议即使在出块时间为 15s 的情况下也实现了了 95%以上的效率，而拥有 25%算力的矿工从中心化得到的益处小于 3%。

费用

因为每个发布到区块链的交易都占用了下载和验证的成本，需要有一个包括交易费的规范机制，来防范滥发交易。比特币使用的默认方法是纯自愿的交易费用，依靠矿工担当守门人并设定动态的最低费用。因为这种方法是“基于市场的”，使得矿工和交易发送者能够按供需来决定价格，所以这种方法在比特币社区被很顺利地接受了。然而，这个逻辑的问题在于，交易处理并非一个市场；虽然根据直觉把交易处理解释成矿工给发送者提供的服务是很有吸引力的，但事实上一个矿工收录的交易，是需要网络中每个节点处理的，所以交易处理中最大部分的成本，是由第三方而不是决定是否收录交易的矿工承担的。于是，非常有可能发生公地悲剧。

然而，当给出一个特殊的不够精确的简化假设时，这个基于市场的机制的漏洞很神奇地消除了自己的影响。论证如下。假设：

1.一个交易带来 k 步操作，提供奖励 kR 给任何收录该交易的矿工，这里 R 由交易发布者设定， k 和 R 对于矿工都是事先（大致上）可见的。

2.每个节点处理每步操作的成本都是 C (即所有节点的效率一致)。

3.有 N 个挖矿节点，每个算力一致(即全网算力的 1/N)。

4.这样，因为矿工有 1/N 的机会处理下一个区块，所以预期的收益是 kR/N ，矿工的处理成本简单为 kC. 这样当 kR/N > kC， 即 R > NC 时。矿工愿意收录交易。注意 R 是由交易发送者提供的每步费用，是矿工从处理交易中获益的下限。 NC 是全网处理一个操作的成本。所以，矿工仅有动机去收录那些收益大于成本的交易。

然而，这些假设与实际情况有几点重要的偏离：

5.因为额外的验证时间延迟了块的广播因而增加了块成为废块的机会，处理交易的矿工比其它的验证节点付出了更高的成本。

6.不挖矿的全节点是存在的。

7.实践中算力分布可能最后是不平均的。

8.以破坏网络为己任的投机者，政敌和疯子确实存在，并且他们能够聪明地设置合同使得他们的成本比其它验证节点低得多。

上面第 1 点驱使矿工收录更少的交易，第 2 点增加了 NC; 因此这两点的影响至少部分互相抵消了. 第 3 点和第 4 点是主要问题；作为解决方案我们简单地建立了一个浮动的上限：没有区块能够包含比 BLK_LIMIT_FACTOR 倍长期指数移动平均值更多的操作数。具体地：

<code style="font-family:Menlo, Courier, monospace, monospace, sans-serif;font-size:13.6px;margin:0px;border:none;background-color:transparent;white-space:pre-wrap;" class="hljs">blk.oplimit = floor((blk.parent.oplimit * (EMAFACTOR - 1) + floor(parent.opcount * BLK_LIMIT_FACTOR)) /EMA_FACTOR)

BLK_LIMIT_FACTOR 和 EMA_FACTOR 是暂且被设为 65536 和 1.5 的常数，但可能会在更深入的分析后调整。</code>

计算和图灵完备

需要强调的是 BTLink 虚拟机是图灵完备的； 这意味着 EVM 代码可以实现任何可以想象的计算，包括无限循环。EVM 代码有两种方式实现循环。首先，JUMP 指令可以让程序跳回至代码前面某处，还有允许如 while x < 27: x = x * 2 一样的条件语句的 JUMPI 指令实现条件跳转。其次，合约可以调用其它合约，有通过递归实现循环的潜力。这很自然地导致了一个问题：恶意用户能够通过迫使矿工和全节点进入无限循环而不得不关机吗？ 这问题出现是因为计算机科学中一个叫停机问题的问题：一般意义上没有办法知道，一个给定的程序是否能在有限的时间内结束运行。

正如在状态转换章节所述，我们的方案通过为每一个交易设定运行执行的最大计算步数来解决问题，如果超过则计算被恢复原状但依然要支付费用。消息以同样的方式工作。为显示这一方案背后的动机，请考虑下面的例子：

一个攻击者创建了一个运行无限循环的合约，然后发送了一个激活循环的交易给矿工，矿工将处理交易，运行无限循环直到燃料耗尽。即使燃料耗尽交易半途停止，交易依然正确（回到原处）并且矿工依然从攻击者哪里挣到了每一步计算的费用。

一个攻击者创建一个非常长的无限循环意图迫使矿工长时间内一直计算致使在计算结束前若干区块已经产生于是矿工无法收录交易以赚取费用。然而，攻击者需要发布一个 STARTGAS 值以限制可执行步数，因而矿工将提前知道计算将耗费过多的步数。

一个攻击者看到一个包含诸如 send(A,contract.storage[A]); contract.storage[A] = 0 格式的合约然后发送带有只够执行第一步的费用的而不够执行第二步的交易（即提现但不减少账户余额）。合约作者无需担心防卫类似攻击，因为如果执行中途停止则所有变更都被回复。

一个金融合约靠提取九个专用数据发布器的中值来工作以最小化风险，一个攻击者接管了其中一个数据提供器，然后把这个按 DAO 章节所述的可变地址调用机制设计成可更改的数据提供器转为运行一个无限循环，以求尝试逼迫任何从此金融合约索要资金的尝试都会因燃料耗尽而中止。然而，该金融合约可以在消息里设置燃料限制以防范此类问题。

图灵完备的替代是图灵不完备，这里 JUMP 和 JUMPI 指令不存在并且在某个给定时间每个合约只允许有一个拷贝存在于调用堆栈内。在这样的系统里，上述的费用系统和围绕我们的方案的效率的不确定性可能都是不需要的，因为执行一个合约的成本将被它的大小决定。此外，图灵不完备甚至不是一个大的限制，在我们内部设想的所有合约例子中，至今只有一个需要循环，而且即使这循环也可以被 26 个单行代码段的重复所代替。考虑到图灵完备带来的严重的麻烦和有限的益处，为什么不简单地使用一种图灵不完备语言呢？事实上图灵不完备远非一个简洁的解决方案。为什么？请考虑下面的合约：

```
<code style="font-family:Menlo, Courier, monospace, monospace, sans-serif;font-size:13.6px;margin:0px;border:none;background-color:transparent;white-space:pre-wrap;" class="hljs">C0: call(C1); call(C1);

C1: call(C2); call(C2);

C2: call(C3); call(C3);


…

C49: call(C50); call(C50);

C50: (run one step of a program and record the change in storage)</code>
```

现在，发送一个这样的交易给 A，这样，在 51 个交易中，我们有了一个需要花费 250 步计算的合约，矿工可能尝试通过为每一个合约维护一个最高可执行步数并且对于递归调用其它合约的合约计算可能执行步数从而预先检测这样的逻辑炸弹，但是这会使矿工禁止创建其它合约的合约（因为上面 26 个合约的创建和执行可以很容易地放入一个单独合约内）。另外一个问题点是一个消息的地址字段是一个变量，所以通常来讲可能甚至无法预先知道一个合约将要调用的另外一个合约是哪一个。于是，最终我们有了一个惊人的结论：图灵完备的管理惊人地容易，而在缺乏同样的控制时图灵不完备的管理惊人地困难- 那为什么不让协议图灵完备呢？

货币和发行

BTLink 网络包含自身的内置通证 BTL，BTL 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。为便利及避免将来的争议期间（参见当前的 mBTC/uBTC/聪的争论），不同面值的名称将被提前设置：

1: 伟
10^12: 萨博
10^15: 芬尼
10^18: BTL

这应该被当作是“元”和“分”或者“比特币”和“聪”的概念的扩展版，在不远的将来，我们期望“BTL”被用作普通交易，“芬尼”用来进行微交易，“萨博”和“伟”用来进行关于费用和协议实施的讨论。

BTL 进入全球每一个国家，可创建 BTL+本国法定数字货币，挖掘 BTLink 公链原生数字资产 BTL。

BTL 市值发行机制如下：

BTL 通证是 BTLink 公链的原生通证，，公链开源协议恒量 2100 万枚。BTLink 全球 IDO42000 个股东算力节点，一期节点 IDO:100USDT，每期股东算力节点 IDO 金额将不断溢价。100U 股东算力节点将在 BTLink 公链写入表达 0.1 枚 BTL 挖矿数据；500USDT 股东算力节点在 BTLink 公链写入表达 1 枚 BTL 挖矿数据。所有股东算力节点可恒久参与 2100 万枚 BTL 验证发行，直至 2100 万枚 BTL 发行完毕。一个旨在为 BTLink 商业生态筹资，30%的资金为来自美国硅谷、瑞士、新加坡、印度等密码学货币开发者支付公链、商业生态等报酬的机制。web3.0 去中心化区块链互联网协议上运行的 BTLink 公链，已经开发了 18 多个月，即将根据全球股东算力节点验证上线。42000 个股东算力节点为 BTLink 原始算力节点，IDO 所得的 USDT，30%用于 BTLink 公链各种商业生态的开发费用，40%为路演营销，30%的 USDT 将添加进 BTL 的 AMM 自动做市机制的全球主流流动性矿池。
8%的 BTL 是 web3.0 去中心化区块链互联网协议，后续 BTLink 公链、和开发各种商业生态应用，以及全球更多密码学参与整个项目的开发费用。10%用于公会治理，8%用于矿池治理（一级算力到达 3 万 USDT 是有效矿池）;4%用于超级节点治理（一级算力到达 1500USDT 是有效超级节点）;70%发行给所有 BTLinkDpos 的股东算力节点，用于全球共识，全球布道!
归属于技术团队的 BTL，每次市值上涨发行的 BTL50%锁仓，被锁仓的 BTL 以 BTL 市值每次上涨 10%-51%，解锁剩余总量的 1%-5%。50%的 BTL 用于 web3.0 协议，BTLink 公链商业生态的开发。
每次发行总量 70%的 BTL 发行给股东算力节点，其中 80%发行给布道共识的股东算力节点，按市值上涨逐步发行给布道共识的 BTLinkDpos 股东算力节点，布道 BTL 的算力节点，每次发行解锁 1-5%的 BTL。
每次发行 70%的 BTL，其中 20%的 BTL 发行给参与股东节点，按市值上涨逐步发行给参与 BTLDpos 的算力节点，每次发行解锁 1%BTL。
每次上涨 10-50%，按已发行 BTL 数量乘以 1%为每次市值上涨的发行量。例:5000 枚乘以 1%等于 50 枚，50 枚乘以 8%等于 4 枚 BTL 发行给技术团队;50 枚乘以 10%等于 5 枚 BTL 用于公会治理;50 枚乘以 8%等于 4 枚

BTL 用于矿池治理;50 乘以 4%等于 2 枚 BTL 用于超级节点治理。35 枚乘以 80%等于 28 枚，按算力值加权发行给布道股东算力节点;35 枚乘以 20%等于 7 枚常规矿工，BTL 加权平均发行给参与节点。
BTLink 公链 GAS 费用 40%加权分配给矿池，10%加权分配给超级节点。

关于 BTLink 的分解

世界投资大师巴菲特，多年一直否定比特币的价值，说比特币是投机炒作，没有创造社会价值。而比特币底层算法是区块代码，他不知道不可篡改加密代码的数据价值，他不知道 web3.0 去中心化区块链互联网的价值。这是巴菲特非常片面的理解，因为他不懂得区块链开源代码，解决了人类诞生以来，通过代码可以无需信任，可以确权的核心价值。规避了人治社会不可掌控的人性，代码治理世界“码制法制社会”。像古老的东方秦帝国统一法制、统一度、量、衡一样。最终可以让人类实现，全球统一的一部《世界区块链代码守则》。让世界更加的平等、民主;让世界更加的可信，和谐。在下一个世纪里，在代码治理的世界下，世界终将实现人类命运共同体，和地球家园!

而 BTLink，它不是简单有价值的 BTL 数字资产，它是集全球商业生态落地应用的全景公链。全世界的实业可以接入的 web3.0 去中心化区块链互联网协议，可以赋能于全世界的商业。同时它又带领世界经济体系，传统实业进入 web3.0 时代。web2.0 互联网的痛点，数据储存在中心化的服务器，数据被中心化公司侵占，数据可篡改，数据可销毁，数据可造假，数据被泄露，个人隐私不安全等一系列问题。同时 web2.0 互联网公司，已经阻碍人类文明的发展。今天，BTLink 打造的 web3.0 去中心化区块链互联网协议，解决了 web2.0 互联网的上述痛点，核心解人类人治的各种弊端，通过不可篡改的的区块链加密代码协议，让每个参与 web3.0 互联网协议的公民，自己的数据，流量运行在区块链上，参与者通过钱包地址，和私钥自己掌控掌管，所有链上的数据、流量、资产、财富等永远属于参与者，无需任何中心化的组织授权，凭私钥可任意转让和继承!

BTLink 区块链商城

区块链商城的推出能做到的就是去中心化!通过两性产品作为数据导流，打造消费购物与区块链技术完美融合的第一平台，助力实体企业快速提高产品销量。同时也让消费者在购物中获得最大的实惠与价值回馈，保障了消费者的个人信息安全。区块链商城利用多种加密、验证方式等手段，保护数据的真实性和安全性，提升用户信任消费和投资消费，能精准获悉用户的消费行为、消费指数、消费素养等点对点服务。区块链商城还内嵌了 DTO 智能合约，利用数字订单、智能合约的可信任机制进行担保交易，买卖家之间的信任成本及交易成本降低，同时去中心化特性去除了第三方机构的参与，极大缩短了时间，提升了效率。营造了诚信加密电商的数字购物新经济平台。

BTLink 加密存储

点对点分布式文件存储协议，可以将所有有相同文件系统的计算机连接起来。传统互联网 HTTP 协议是搜索域名地址，但是 BTLink 是搜索内容地址。BTLink 用 Web3.0 协议颠覆 HTTP 协议的方法，可以让网络更快更安全，充分保障沟通隐私。
BTLink，就是让文件分布式存储和读取。现在网上的所有信息，都是存在服务器里，万一服务器挂了呢，我们搜索信息就搜不到了。为了防止这样的事情发生，BTLink 技术就把文件打碎，分散地存储在不同的硬盘里，下载的时候，再从这些散落在全球各地的硬盘里读取。其实用过 BT 下载的人会发现，BTLink

其实就是一种 BitTorrent 协议，开发团队对 BitTorrent 协议稍微升级了一下。
传统存储 VS 分布式存储
传统存储：
单点故障瘫痪整个网络
通信依赖主干网络带宽成本昂贵
存储媒介易被垄断数据无法自主
数据上传与下载速度慢
存储空间升级难扩容存储成本昂贵
分布式存储：
聚合亿万节点：系统稳定可靠
加密碎片数据：数据安全无忧
弹性存储容量：可扩展性能高
就近多点传输：上传下载极速
去中心数据库：打破数据垄断
区块技术加持：数据溯源确权

本地存储一向以可靠性高、稳定性好，功能丰富而著称，但与此同时，本地存储也暴露出横向扩展性差、价格昂贵、数据连通困难等不足，容易形成数据孤岛，导致数据中心管理和维护成本居高不下。
随着云计算的发展，特别是互联网企业云数据中心的成功实践，分布式存储（云存储）替代传统存储阵列（本地存储）的呼声日益高涨。相比于本地存储，分布式存储不仅提高了存储空间的利用率，还实现了弹性扩展，降低了运营成本，避免了资源浪费。

依靠 BTLink 发布的信息不会突然在服务提供商或托管网络的突发事件中消失，安全性增加，BTLink 没有中央分发系统、速度也很快。

BTLinkF 所具备的优势，恰好能解决传统中心化云储存数据易泄露、硬件易损坏、修复能力弱、安全性低，并且随时面临运营终止风险的问题。

分布式存储通过 BTLink 底层协议，将数据库复制成多份，保证冗余性，再分割成多个小部分，分散存储在网络众多节点上，这样只要足够多的节点运作正常，数据就是安全的。

BTLinkVR、AR、XR 虚拟场景生态

虚拟现实（VR）是一种由计算机和电子技术创造的新世界，是一个看似真实的模拟环境，通过多种传感设备，根据用户自身的感觉，使用人的自然技能对虚拟世界的物体进行考察或操作；同时提供视觉、听觉、触觉等多通道的信息，使用户通过视、听、摸等直观而又自然的实时感知，并使参与者沉浸于模拟环境中。虚拟现实技术在最近十年里获得了极大的发展，这主要归因于计算机软、硬件条件的飞速发展。虚拟现实技术中的虚拟场景建模工作是研究的核心问题。

建模即建立模型，建立系统模型的过程，又称模型化。建模是设计的重要手段和前提。设计建模是设计初期要做的工作，建立起一个框架，就像建房先要画出平面图，装修要有装修图一样。只有建模完成了才能一步步来完成设计。

后期裸眼全息投影是一种无需配戴眼镜的 3D 技术，观众可以看到立体的虚拟人物，第一阶段实现人类“永生”，可以离世的亲友在 web3.0 的元宇宙世界里“复活永生”，可以和在世的亲友们随时交流互动。这项技术在一些博物馆应用较多，后期我们 BTLink 将完全运用全息立体投影技术来实现人与人的互动，交流。而是投影设备将不同角度影像投影至一种国外进口的全息膜上，让你看不到不属于你自身角度的其他图像，因而实现了真正的全息立体影像。全力运用生态实行在合成时可自由调节时间线， 为复杂的特效图层合并多个时间线。

BTLink 生态链游戏互动生态

**GameFi = DeFi + NFT + Game** 其高度去中心化特点和规则，**让玩家实现游戏资产私有化，安全化，透明化。游戏中玩家所有的一切道具、资源甚至角色都是可货币化的，可供玩家之间自由交易来赚取收益。**

1. Play-to-Earn

Play-to-Earn，简称 P2E，是 GameFi 中的最重要的元素， “边打边赚”是 GameFi 与所谓传统游戏的最大分别。

传统游戏内的钱（比如魔兽世界里的金币，CS 里的钱，王者荣耀里的点券、钻石），只能在同一款游戏中使用，无法将其换为现金。

GameFi 游戏，玩家所赚到的游戏代币就像普通加密货币一样可以流通市场，能够换为现金或其他币种。玩游戏要赚到钱，才能令玩家继续参与及吸引更多玩家加入，变相每个细项的营运模式相当重要。

另外，“边打机边赚钱”本身就收极佳宣传效果，发行商只要控制好加密货币发行量，若果价格急升的话，自然就会吸引大批用户，变成忠诚玩家，一起赚币，同时省却大量推广费用；游戏发行商可以透过交易抽取佣金，也可赚取收益。结论是，只要建立好游戏生态圈，令“元宇宙”顺利运作，可造就多方共赢局面。

道具都是 NFT 代币；将道具铸成 NFT 有三大特性：真正由玩家拥有、每个 NFT 都独一无二更具稀有性、除了在游戏内置的市场出售也可以在其他市场（例如：Opensea ）出售。

3. 抵押道具

基于上述的属性优势，部份游戏道具 NFT 可以成为其他 DeFi 平台的抵押品，让玩家抵押自己的游戏资产 (NFT) 来借贷；又或是在其他 Dapp 应用上，通过质押 NFT 资产或游戏代币提供流动性，通过抵押赚钱（如流动性挖矿、质押理财一样）。

4. DAO 管治

一般游戏代币在 GameFi 最了是奖赏，还是游戏的管治代币 (Governance Token) ；持有 Game token 代币的人可以通过投票方式，为游戏进行升级或提出改进方案。DAO 组织管理是去中心化应用的普遍做法，令玩家不再单纯只是玩家的角色， 甚至有权决定游戏未来的发展。

BTLink 去中心化交易所

去中心化的核心就是“去托管”，去中心化交易所的核心是“资产去托管”。也就是说，在交易的过程中，没有任何人或者说一个中心化的机构能够动用你的资产。去中心化交易所与中心化交易所不同，主要体现在技术与治理两个方面。

从**技术角度来看，去中心化交易所是通过链上的智能合约来实现交易的**。而传统的中心化交易所是在链下进行交易。

从**治理角度来看，去中心化交易所的治理带有开放和社区驱动的属性。**而中心化交易所的治理模式与传统公司相同。

当使用不同的中心化交易所时，需要重复进行账号注册与 KYC 认证。而使用去中心化交易所则不存在这个问题：你只需要有一个钱包就能使用不同的去中心化交易所。即**无需注册，一个就够。**

以下是区块天眼上排名前五的去中心化交易所：

**应用**

交易流程

1.开户:注册获得新的地址和密钥,用户掌握私钥,拥有对资产的绝对控制权,一旦丢失无法找回。

2.充值:充值比较简单,直接由钱包地址充值到去中心化交易所的新地址

3.交易:当发起交易时,直接执行去中心化交易所的智能合约来完成交易,整个过程用户一直拥有着币的所有权,去中心化交易所无掌控权。

4.提现:用户无需授权，人工审核，从去中心化交易所转账到自己钱包地址。

产生费用使用 BTL

1.充值时,从用户钱包地址充值到交易所的新地址,要使用 BTL 作为手续费。

2.交易时,去中心化交易所也会收取手续费,手续费直接从交易的币种里扣除。

3.提现时,交易所地址充值到用户钱包地址,会产生相应使用 BTL 作为手续费。

**优势**

1.去中心化交易所模式简单,主要是撮合交易,并不托管用户的资产,杜绝了交易所监守自盗的可能性。

2.与中心化交易所最大的不同在于,所有的这一切都通过智能合约来实现,将资产托管、撮合交易、资产清算都放在区块链上。

3.用智能合约来实现去中心化去信任的交易机制,解决了中心化交易所因人为因素产生的内部运营风险、商业道德风险、资产盗用等严重影响用户资产安全的风险。

4、解决现在去中心化交易所，无 K 线图、无币价挂买挂售、无买多买空合约等功能。

5.用户的托管资产可以自由转移无需任何人审批,也不用担心黑客盗取、丢币等问题发生,安全上具有足够的保障。

BTLink 加密社交金融

每条消息都经过加密处理，因此只有发送方和接收方才能读取，即使是黑客也无法从中拦截，由于使用的开源加密。可以让专家测试并借此发现问题，这样可以让这个程序更加的安全，这款软件也是支持自动删除已发送的信息，可以防止别人在拿到你的手机后泄露你的聊天记录

适用于 ios，安卓和 windows phone、pc 和苹果电脑等，在最新的加密技术中，外部默认就开启了端到端的加密功能。发送的消息，以加密代码的形式传输到对方的手机上，只有收件人的手机上安装了这款聊天工具，并且通过软件内置的加密密钥，才能将加密代码转换为可见的纯文本信息，加密密钥仅存在用户的设备上，任何的内容都不会存储在外部的服务器上，因此没有人、甚至连外部都无法阅读你的信息。还提供阅后即焚，可以给会话中的消息设置一个自动销毁的时间。

可以加密转账，加密聊天，视频传播。应用于各大生态版块，如元宇宙，NFT，游戏等。

BTLink 跨链

跨链（Cross-Chain）即是容许加密货币资产，跨越不同的区块链使用和保存。

BTLink 跨链桥是连接各个区块链、进行资料和资产传输必备的「桥」，使得不同加密生态系统之间能够进行互动，令不同的区块链网路可以相互兼容。

这条「桥」不是物理意义上连接不同位置的伺服器，而是一些协议和技术，令到使用不同共识机制的区块链间，能够互相转移资料和资产。

当投资者在不同区块链上进行投资、质押、GameFi 等等活动时，会受限于不同区块链使用各自的共识机制，无法整合资产。

BTLink 跨链功能种类一、链对链桥：链对链转移资产

链对链跨链桥（Chain-to-Chain Bridge）主要作用是支援两个主要区块链之间的资产转移。

例如 Polygon 官方推出的桥 PoS Bridge，主要支持以太坊和 Polygon 之间的跨链；Avalanche 官方推出的 Avalanche Bridge，主要支援 Avalanche 和以太坊链 ERC-20 标准的跨链资产转移。

BTLink 跨链功能种类二、多链桥：任意链间转移资产

多链桥（Multi-Chain Bridge）能够跨多个区块链转移资产，可以被应用到任何 Layer1 或 Layer2 区块链上。

BTLink 跨链功能种类三、专用桥：特定生态系统间转移资产

专用桥（Specialised Bridge）专注在特定的生态系统，专门支援资产在特定区域之间的转移。

由于这些桥的专用性，专用桥通常可以提供更快、更便宜的跨链服务。例如 Hop Protocol 的跨链桥方案是 Rollup-to-Rollup 的通用资产桥，专门实现 Layer 2 网路之间和以太坊主网之间的资产转移。

BTLink 跨链功能种类四、打包资产桥：打包转移资产

打包资产桥（Wrapped Asset Bridge）专门用来将非原生资产转移到不同的区块链上，方法是在目标链上创建出打包资产(wrapped assets)。

例如用以太坊上的 Wrapped Bitcoin（WBTC）为例，就是由托管方持有 BTC，再根据持有的 BTC 量，在以太坊上用 ERC-20 标准，铸造 WBTC。

BTLink 跨链功能种类五、数据专用桥：跨多链任意传输数据

数据专用桥（Data Specific Bridge）是专门为跨多个区块链传输任意数据而设计的互操作性协议，这些协议通常会成为 dApps 的基础层，令 dApps 能够实现跨链组合。例如 Celer 的 Inter-chain Message Framework 和 IBC。

公证人机制（Notary schemes）

侧链 / 中继链（Sidechains / relays）

哈希锁定（Hash-locking）

分布式私钥控制（Distributed private key control）

BTLink 跨链技术一、公证人机制：第三方确认资产转移

公证人机制（Notary schemes）是通过寻找一个公正独立的第三方来作为两条链之间的中介，由公证人来协助验证交易。

公证人会负责确认资产在两条链上的状况，并且传递资讯。例如当需要将 100 USDT 从以太坊转到 BSC 时，公证人会确认这 100 USDT 的价值，并且把这项资讯转传到 BSC 上，确认 BSC 上收到 100 USDT。

第三方公证人，可以是中心化的存在，或者去中心化的节点，种类略分为以下三种：

中心化公证人

选择单一节点或是中心化组织作为公证人，不过公证人一旦受到攻击或遭逢意外，就很容易停摆。

多重签名公证人

需要多位公证人，在所有公证人都完成签名、达成共识之后，才能够完成跨链，更加去中心化和安全。

分布式签名公证人

需要多位公证人的参与。机制会随机抽取部分公证人，并在公证人完成签名后加密完成私钥。这种机制涉及密码学的公私钥，所以比起多重签名公证人机制，更加复杂和安全。

BTLink 跨链技术二、侧链/中继链——接驳主链间转移资产

侧链（Sidechains）：是依附在公链旁、一条规模较小的区块链，可以将其视为公链的一个外置硬件。

侧链能够接收并读取主链交易的资料与数据，并将透过「锚定」的方式锁定要验证的内容，并将侧链&主链上的资产双向锚定。当交易资料通过验证，主链资产将被锁定，然后在侧链上释放等额资产，原理颇像跨国的货币兑换。相反，当侧链上的资产被锁定时，主链上也会释放相对应价值的资产。资产实际上并没有被转移，而是被锁定和重新释出。

中继链（relays）：中继链与侧链最大的差别，在于侧链是依附在主链底下，与主链关系紧密；而中继链则是与其他公链对等、平行，并不属于任何公链。中继链则类似公证人机制与侧链结合，中继链即可连接不同公链的资料调度中心，以第三方公证人的身份，验证不同公链间的交易资料。在读取和验证公链上的资料后，中继链锁定原链上的资产，然后在目标链上释出等值资产，达成资产锚定的功能，确保两边的交易资料对得上。

BTLink 跨链技术三、哈希锁定——私钥函数转移资产

哈希锁定（Hash-locking）听起来很难懂，但实际只是在跨链的模式上，多加了一重密码学设计，以经过杂凑函数加密处理的验证机制，去处理跨链资讯对接。运作流程如下：

1. 智能合约锁定使用者在 A 链上的资产

2. 智能合约用随机产生的数字和杂凑函数产生一组私钥

3. 使用者于规定时间内，在 B 链上提供正确的私钥

4. 智能合约在 B 链上释放出相对应价值的资产，完成跨链。

如果交易失败，或是未能在时间内提供正确的数字，A 链上锁定的资产会自动解锁，返还给使用者。

BTLink 跨链技术四、分布式私钥控制——多方分散保管私钥

分布式私钥（Distributed private key control）运用用智能合约，投射原链上的资产到其他不同的链上，同时产生一组控制这些资产的私钥。

这份私钥会分散由不同的机构或节点保管，达成去中心化，保障资产安全。当使用者需要转移资产到另一条公链时，就可以通过这组私钥，在不同链上锁定与解锁和解锁资产。

以资产转移方式分类跨链技术

至于跨链的本质技术又如何，粗略可分为以下三类转移资产的方式：

一、锁定+重新铸造

这个方式是锁定原链上的资产，并且在目标链上重新铸造资产，例如 Polygon 的 PoS Bridge、Avalanche 的 Avalanche Bridge (AB) 和 Wrapped BTC (WBTC) 等。

情况就像把你将货币 A 放在国家 A 的一个银行金库里，而获得存放认证后，就能在国家 B 换领同价值的货币 B；当你再次需要动用货币 A 时，你只需要把国家 B 当中尚有的资金归还，就可以重新使用国家 A 当中对等价值的货币。

二、销毁+重新铸造

这个方式是销毁原链上的资产，并且在目标链上重新铸造资产。再以上述例子而言，就等于你先注销国家 A 的货币，然后在国家 B 再申请同等价值的货币，然后回到 A 国家时则相反操作。

三、原子互换

至于所「原子互换」，则是更进一步，不需要像上述两种方式般销毁或是锁定，直接透过已认证的智能合约机制，转换两种资产，也就是直接以 A 货币，换领 B 货币。

解决 web2.0 数据存储在中心化的服务器上，社交账户的数据流量不在归属平台公司。因为所有数据流量运行在区块链上，用户用钱包地址注册，凭私钥掌握社交账户在区块链上的数据，凭私钥可赠予、继承任何人。

支持 BRC-20 协议、BRC-721 协议，企业、个人等可一键发行企业链和个人链，可在该专有链创建各种应用，发行专有代币和通证。

综述：去中心化应用

上述合约机制，使得任何一个人能够在一个虚拟机上，建立通过全网共识来运行命令行应用（从根本上来说是），它能够更改一个全网可访问的状态作为它的“硬盘”。然而，对于多数人来说，用作交易发送机制的命令行接口，缺乏足够的用户友好，使得去中心化成为有吸引力的替代方案。最后，一个完整的“去中心化应用”，应该包括底层的商业逻辑组件【无论是否在 BTLink 完整实施，使用 BTLink 和其它系统组合（如一个 P2P 消息层，其中一个正在计划放入 BTLink 客户端），或者仅有其它系统的方式】，和上层的图形用户接口组件。BTLink 客户端被设计成一个网络浏览器，但包括对“BTL” Javascript API 对象的支持，可被客户端里看到的特定的网页，用来与 BTLink 区块链交互。从“传统”网页的角度看来，这

些网页是完全静态的内容，因为区块链和其它去中心化协议，将完全代替服务器来处理用户发起的请求。最后，去中心化协议可以自己利用某种方式使用 BTLink 来存储网页。

最后，致敬伟大的万维网之父:蒂姆•博纳斯•李，致敬伟大的区块链之父:中本聪!