YGGDRASH

Trust-based Multidimensional Blockchains
& Internet re-designed by blockchains

White paper (ver 0.22.2)

YGGDRASH
Trust-based Multidimensional Blockchains
& Internet re-designed by blockchains

白皮书（0.22.2 版本）

*本文件只作为提供一般信息用途，白皮书所载内容不作为对特定公司或个人的交易条件规定的解释，且不会对未与 AKASHIC FOUNDATION LTD.缔结法律关系的第三方行为（第三方间交易等）负有任何责任。
*本公司拥有本文件的知识产权，未经允许进行分发或盗用时，将追究法律责任。
*在编写本文件时，假定读者已经拥有了关于区块链的基本常识。
*如有疑问，请咨询 info@yggdrash.io。

前言

我们畅想的未来

我们的未来正变得越来越复杂，产生越来越多的交易和数据。
和现在一样，未来对我们最重要的要素仍然是数据管理。
但是想象一下，如果数据体系依旧像现在一样，将所有数据整合在一起，通过一点管控连接所有的各个支点，会发生什么事情呢？这样做，无疑是将所有危机都集中在了一起。
如果人们为使用自己的资产，或是维护自己的生命，就把所有数据都放在一个自己信赖的地方，这样做到底是不是正确的决定？是不是最佳选择呢？
如果在某一瞬间，那个支点突然不能工作了，怎么办？如果突然发现了有人利用自己珍贵的信息，怎么办？以后还能继续相信该体系吗？这是一个要不要继续相信一个无法保障安全体系的问题。

网络被称作是信息的海洋，区块链即使无法改变所有内容，但还是可以改善社会的诸多问题。因此，我们需要有一个平台帮助我们迈出面向未来的第一步。
所有区块链都有各自的监管体系。如比特币和以太坊就因各自追求的目标和方向不同，其解决问题的想法也必然存在着差异。

YGGDRASH 意在建立一个既支持这种思维上的差异，同时又能提出解决办法的平台。

区块链改变了很多理念。但当我们走进区块链，就会发现每个区块链在解决问题方面都存在各自的困难。之所以会出现这种困难，是因为网络分散或网络用户将各自的网络集中在一个区块链，所有交易结果集中到一个区块。

这导致了网络分散化和信息集中化，这也是区块链性能的临界点。一个区块链的缔结速度再快，为了保障多人同时登录，也一定会出现瓶颈现象，这是 p2p 网络要解决的根本课题。

许多区块链项目依旧在努力解决这一问题，而我们将作为区块链世界的先驱贡献出自己的力量。

Team Yggdrash

1. 概要

1.1 Why, Another, Blockchain? (为什么, 另一个, 区块链?)

1.1.1 交易处理性能, 区块检验节点的利己性竞争及区块链的同步速度问题

交易速度（TPS）/处理量（Throughput），即交易处理性能是什么？这是测定每单位时间一般可以处理多少交易的数值。现在区块链正被激增的交易数据和 DApp 数据困扰。如果是既有的中央化服务器方式，就可以根据通信量增加，增设服务器解决问题。然而，区块链是利用 P2P 网络资源进行演算工作，因分散化的 DB 环境及处理性能，与既有方式不同，存在只能在速度方面放缓的限制。另外，如果节点间的协议过程增加，问题解决起来就会愈发复杂。

和区块链处理性能密不可分的就是区块检验节点，即挖掘者的经济奖励。作为区块链开端的比特币就坚信根据数学证明和游戏理论可以吸引挖掘者自发参与其中，同时通过相对应的奖励可以形成透明且稳定的生态体系。但是，呈线性・爆发性增加的交易环境一出现，以收益性为基准的所有交易和 DApp 就变成了强行排序的利己式区块检验。而且，就算出现了可以创造高价值的交易，在需要支付小额手续费时，推迟运行或是永久不能运行的情况屡见不鲜，这就是今天区块链的现实。

在区块链世界还未被广泛讨论的问题是区块链容量增加和速度同步。区块链带有基本区块与区块间连接的结构，根据交易的增加，全部区块的容量和区块同步时间就不得不持续增加。比特币以 2012 年为基点，区块容量和区块同步时间每年平均增加 2 倍，到 2018 年 2 月为止，比特币的容量为 150GB，区块同步时间平均为 14 天。这不仅成为阻碍普通人加入区块链的因素，还导致分散的区块链向中央化这一错误方向的转变。现在，区块链需立即解决眼前处理性能的问题，或者在第 4 产业，让区块链适用于小型 IoT 设备的话，就必须解决区块链容量和同步速度问题。

1.1.2 比特币的临界点和现况

区块链 1.0 时代，比特币初次登场时就受到了广泛关注，原因就在于其基于去中央化的安全性、快速转账，以及几乎为 0 的手续费。然而现在情况又如何呢？“超快的转账速度”因大量交易延迟和未承认问题成为诟病；“几乎为 0 的手续费”在最近 3 个月已经涨到了平均 55 美元，约合 6 万韩元，这使得比特币根本无法用于日常结账或小额交易。为什么会发生这些问题呢？这都是因为公共区块链本身 1）未能解决分散 DB 的处理速度，2）分散 DB 的生成/共享节点的经济奖励设计失败。

以下是比特币正面临的实际情况。

“51 分"
最近 30 天内，比特币交易完成所需的平均时间（BlockchainInfo.com）

“55 美元"
以最近 3 个月为标准，1 比特币平均交易手续费（blockchain.info/charts）

“214,817”
目前在比特币网络，未能进入区块正四处漂流的交易件数（blockchain.info/charts ）

“150GB & 14 天”
目前比特币的所有区块规模和区块同步所需时间（bc.daniel.net.nz）

“30.14 太瓦”
比特币一年的耗电量（虚拟货币专门在线媒体 Digiconomist）
30.15TW 已经超过了爱尔兰整体耗电量数值（年耗电量 25TW）。

1.1.3 以太坊的临界点和现况

区块链 2.0 时代的以太坊，它不再是单纯的货币，同时还提供合约、SNS、电子投票等多样的 DApp 的平台。但它 1）在以太坊的区块链上同时会引起所有 DApp 记录和处理扩张性问题；2）出现了和比特币相似的经济学的奖励限制情况。

以下是以太坊正面临的实际情况

“Crypto Kitty"

11 月 28 日，可以买卖虚拟猫的以太坊 DApp——Crypto Kitty 大受欢迎，导致以太坊网络 pending transaction 件数比平均增加了 6 倍，以太坊网络一度陷入麻痹状态。

“以太坊 gas（gas,手续费）问题”
以太坊因图灵完整性（Turing-Completeness）、安全等原因设计了用户缴纳 gas 费用。这是传统中央化服务用户很难接受的手续费政策。（EOS 的代币政策更合理）

“DApp 间相互联通时，手续费支付问题”
现在在以太坊上已发布无数的 DApp，当这些 DApp 相互联通形成一个服务运作时，（各 DApp 实施独立手续费政策时）用户为使用其中一个服务，向甚至不了解的各个 DApp 每次支付手续费（当然，如果各项服务达到商用化水平，现有的大部分 DApp 经过融合，可能会形成一个结构更加完整的 DApp）。

“低水准的 DApp 无法运行，或永远无法运行的问题”
以太坊是支付手续费的用户或运行相应服务方的见证人。见证人会优先检测收益性高的 DApp，这就导致收益低的 DApp 几乎或是根本不能运行。

“攻击者费用和使用者费用问题”
因无法区分攻击者和使用者，对两者实施同一手续费政策而导致的问题。本应降低使用者的手续费，提高攻击者的手续费，但现在进退两难。

“650GB & 8 天”

现在以太坊整体区块规模和区块同步所需时间（bc.daniel.net.nz）

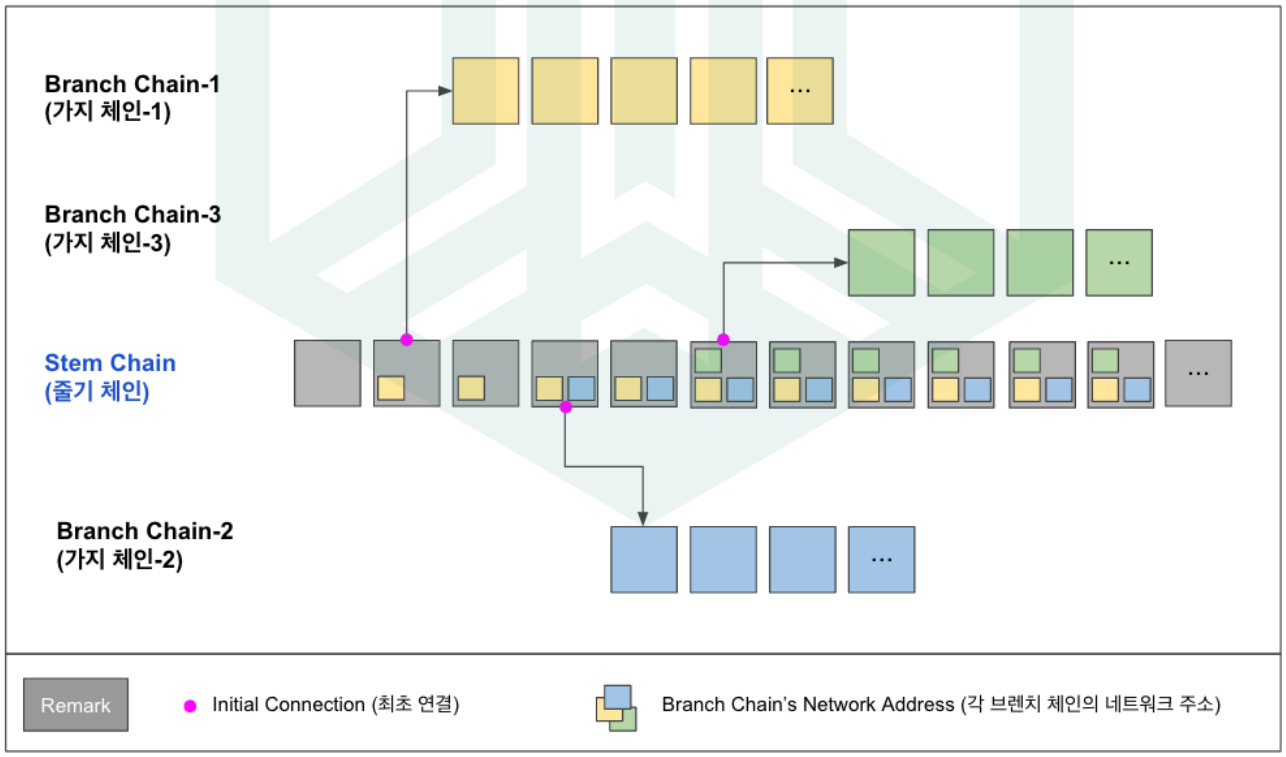
2. YGGDRASH 介绍

包含世界树之意的 YGGDRASH 是连接所有区块链的通道。
YGGDRASH 项目以信赖为基础，目标是连接所有区块链（Trust-based Multidimensional Blockchains）及通过区块链重组网络上的所有服务（Internet re-designed by blockchains）。

Yggdrash 词源
Yggdrash = Yggdrasil + Hash
Yggdrasil 是源自太初之树、世界树、神坛树等传说的大树，是在人世间、天上世界和地下世界起连接桥梁作用的世界树。

2.1 YGGDRASH 的构成要素

YGGDRASH 大体有干链（Stem Chain）和支链（Branch Chain）构成，干链可为各支链提供相互通信及融复合的环境。



2.1.1 干链(Stem Chain)

干链是 YGGDRASH 的基本链，是载有所有支链信息的信息集合体，也是一条通道。干链只保存各支链的最少信息，如地址等，因此可保障最优质的交易处理性能和扩张性。此外，因保存了各支链的地址，不仅可以连接各支链，还可管理各支链的 Life-Cycle（生成/变更/废除）。

2.1.2 支链 (Branch Chain)

支链是一个 DApp，同时也是一个区块链。因为支链本身就是区块链，自然可以选择自己想要的协议运算法则，形成专属区块链。结果就是我们的每一个支链都达到了 DAO(Decentralized Autonomous Organization)）水准。

可以把支链看作侧链。这部分作为一个非常重要的概念，现有的各链之间都需要使用像 Atomic Swap 等人为技术进行连接，但 YGGDRASH 将支链与干链相连，同时又能保障各支链间自然连接，相互参考，这样就形成了一个可以在各支链间轻松交易资产的环境。
此外，支链由各自独立的区块链运营，这样就可以保障即使某一支链的交易超负荷，或是出现故障，也完全不会产生任何影响。

以下将介绍支链类型。

1. 永恒支链**(Immunity Branch Chain)**
YGGDRASH 使用的支链，不消耗 YEED，也不会在目录上清除

2. 消耗性支链**(Mutable Branch Chain)**
用户生成的支链，每一定期间消耗 YEED

3. 即时支链 **(Instant Branch Chain)**
用户生成的支链，不消耗 YEED，只存在一定时间的支链
（只有信任度达到一定程度的用户才能生成该支链）

4. 测试, 隐私支链**(Test, Private Branch Chain)**
未与 YGGDRASH 连接的支链，用于测试和隐私的支链
（干链无法感知该种支链，只有知道该支链信息的用户群体才可共享或自身保有）

2.1.3 主要支链(Important Branch Chain)

1) 内部货币链**: YEED**

在我们居住的现实世界，需要货币的理由是什么？虽然货币的实质目的是交易的手段，但也可以认为是维持社会的一种巨大力量，换句话说，货币是一种工具。YEED 是 YGGDRASH 的货币，是维持 YGGDRASH 网络的一种工具。虽然也是交易的手段，但最重要的目的是连接并维持与 YGGDRASH 网络相连的无数区块链网络。

通常，新生成的区块链不会在 YGGDRASH 的干链上登录。将自身区块链与 YGGDRASH 网络相连，就要使用 YEED。随着时间的流逝，支付的 YEED 也会一点点被消耗掉。

新加入的支链，在参与 YGGDRASH 网络的同时，将更容易分享多样的区块链资源和服务以及结交合伙人。 另外，只要自己构建的区块链服务足够优秀，自然就可以吸引更多的合伙人和用户。

2) 信任度评价链：生命之水（Sacred Water）

在加密货币中，用户为什么要支付网络手续费呢？大部分加密货币收取网络手续费的原因如下。

1.为了给挖掘者提供区块采掘的奖励。另外，因区块规模资源有限，所以挖掘者也努力在区块内搭载更多高手续费的交易。

2.为了拦截恶性用户。如果无需支付网络手续费，那么恶性用户就可以无限制地进行大量交易，造成网络瘫痪，或将毫无意义的信息登录到区块链上。

那么要如何解决这样的问题呢？将交易内容或数据上传至区块链，就像脸书用户在脸书上写文章一样。

时间对任何人来说都是最公平的资源，YGGDRASH 基于这点，对可信度进行测评，为有利的用户提供优惠，同时限制恶意的用户。在 YGGDRASH 网络的时间越长，所作有利的事情越多，就可以提高可信度，得到各种各样的优惠。优惠之一就是手续费。
信任度分数越高的用户在使用我们的网络时，就不需要支付手续费。这和银行的高信用用户在使用银行基础设施时可以免手续费是一样的道理。
当然，对高信任度用户除了手续费之外还可以提供的更多。
例如，信度度最上位参与者 在发行新的 YEED 时，可以获得一定比例的货币。换句话说，就是会得到与自己贡献等值的补偿。

在我们居住的现实世界，信用是可以用来交易的资源吗？我们信任的人不可能统一的向每一个人平等地赋予自身的信任。
达到一定信任度的人存在通过消耗部分信任度，按一定比例赋予他人的政策。信任转移将通过部分转移时根据共同体协议进行发展・改善。

想积累 YGGDRASH 的可信度，就要为 YGGDRASH 网络做贡献，投资大量时间。
但是，如果使用者以破坏网络为目的积累信任度，被监视系统或网络参与者发现，就会扣除信任度。
此外，依据信任度政策可制定免手续费优惠消失，YGGDRASH 资源不能活用，或不能积累信任度。

在 YGGDRASH 最重要的资产不是 YEED，而是可以给予无数人优惠的可信度。YGGDRASH 将创建向更多参与者提供更多优惠和权力分散及共同成长的健康的区块链生态体系。

3) 信用值生成链：生命水之泉（Sacred Water Fountain）

网络参与者在信用值生成链上实现信用值生成，其运算法则设计为对 YGGDRASH 网络的贡献越大，信用值就会越高。在相应时间，如果不运营节点，就无法得到信用值。另外，我们还设有监视和处罚系统，以应对恶意获取信用值的用户。

2.2 YGGDRASH 的优势

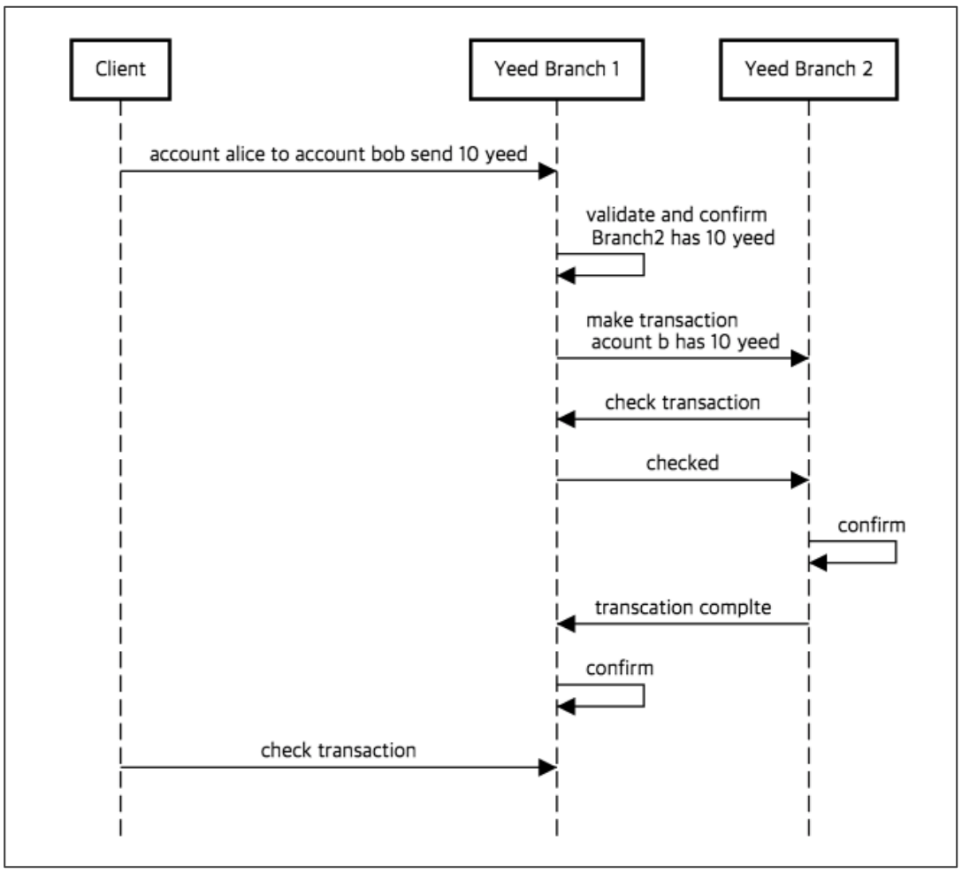
2.2.1 解决智能合约数据容量问题

以太坊的智能合约提高了区块链分权化的价值。
智能合约将现实社会不能实现的无数交易匹配交易规则实现自动化，打造出一个透明且高效的世界。但是随着区块链搭载越来越多的智能合约，也就遇到了容量的临界点。

如果在实际开发缔结智能合约 APP 的过程中，无法解决容量问题，最终结果就我们预想的商业不能现实化。那么该如何解决这一难题呢？答案就是只将智能合约的完整信息上传至区块链，通过其它渠道获取二进制文件，就可以解决智能合约的容量限制。同时可解除使用智能合约的语言限制，开发智能合约的门槛也会明显降低。

2.2.2 通过区块链网络分片（Sharding）提高处理性能

YGGDRASH 可利用多维区块链特征，实现网络分片。



首先，想要进行分片的支链应全部拥有相同的监管，各支链也应具备与分片相关的其它支链信息。

相应事例是 2 个支链进行分片的事例。处理分片的标准是以各支链的账号为基准（例如_单数、双数）进行了假设。

如上所示，2 个支链进行分片时，如果是 Yeed 支链 1 向 Yeed 支链 1 移动的话，那么就和平时一样，只会发生 1 个交易；如果是 Yeed 支链 1 向其它支链移动的话，Yeed 支链 1 就会以资产托管交易状态生成 Yeed 支链 2 产生的 2 个确认。

对此可作如下表达。

```
sharding effect = same branch 50% + other branch (3) 50% = branch sharding count / 2
```

在相应例题中，是 2 个支链进行分片的情况。如上所示，在进行分片时，分片的写入性能（交易处理性能）是将一个支链进行交易的性能进行了提升，而 3 个以上支链进行分片时，性能也会逐步提升。

预测 YGGDRASH 的单一支链性能约为 1000TPS 到 10000TPS 之间的话，通过区块链网络分片可提升处理性能。
因相关技术原因，YGGDRASH 可构建大量微支付交易处理的相关服务。

2.2.3 使用阿卡西系统-BRA（Block Reassembling Algorithm）提升节点同步速度

如今，构成主网的大部分区块链正在提供像智能合约等在自身区块链上可灵活运用各种技能的全节点（钱包）。但是，大部分的加密货币用户都是利用加密货币交易所或轻客户端节点（钱包）服务进行加密货币交易及使用智能合约。因为建立全节点的过程过于繁琐。其中最大的限制条件就是所有区块下载，同步化的时间的，经济的问题。

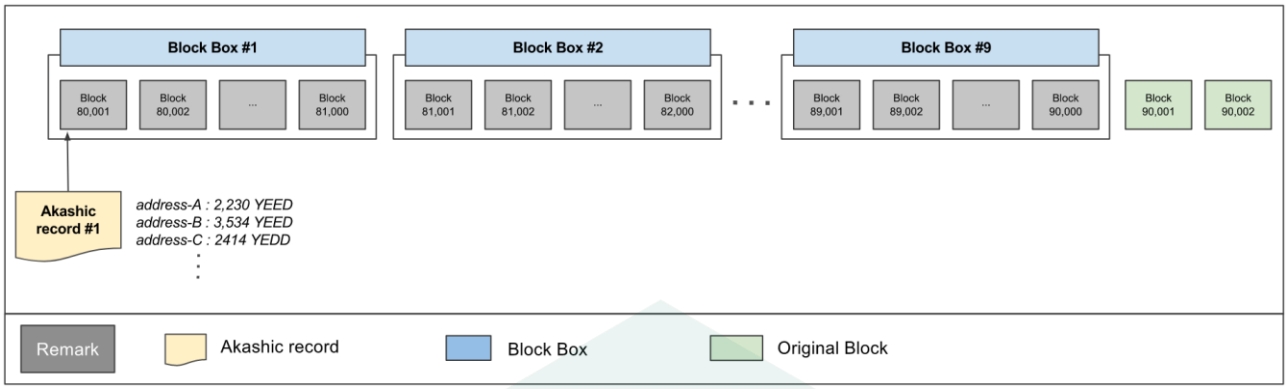
比如：比特币区块同步时间约为 14 天，以太坊也需要大概 8 天的时间（480 万区块/2018 年 1 月基准）

想构建其它区块链平台全节点的人会因为该问题，不是从初始块进行同步，而是选择通过 P2P 网络获取已经共享在网络上进行过一定程度同步的钱包，以此降低同步时间。但是从 P2P 网络的特性上（种子等）来看，所得钱包的信任度并不能得到保障，极有可能遭受病毒等危险。

YGGDRASH 意在通过区块重组演算（BRA：区块重组演算 Block Reassembling Algorithm）实现高效且安全的区块同步。

区块重组演算由以下 3 个要素构成。

- 阿卡西记录（AR：Akashic Record）：N 个区块转移、所有交易结果值的集合
- 区块盒子（BB：Block Box）：N 个区块被装在一个盒子中的区块集合



- 区块（OR：Original Block）：一般区块链的区块

阿卡西记录是从创世区块到特定时点区块的所有交易结果（所有账号交易的结果值）的储存集合（data checkout），区块盒子是将几个区块装在一个盒子内的区块集合。

为具体实现 BRA，会把制定 AR 和 BB 的政策将结果值杂散，并储存在区块上，而实际 AR 和 BB 的二进制数据将被记录在 YGGDRASH 文件共享网络上。利用实际 BRA 对节点进行同步时，在 YGGDRASH 文件共享网络并联下载相应区块数据后，与储存在 YGGDRASH 区块上的 BRA 散列值进行对比，保障文件的完整性和安全性。

YGGDRASH 在不破坏区块链优点的同时，努力让所有网络参与者都能够更容易地参与到区块链网络中来。
另外可以根据新生节点进行全节点同步的选择，扩展使用 BRA。

下面将通过事例，为大家说明在使用 BRA 后，实际同步速度可以提高多少。

- Scenario

  - 现在，在区块高度为 489002 的情况下，让我们假设有新节点加入。

- BRA 运营政策

  - AR（Akashic Record）：每 100000 个区块保存阿卡西记录结果值
  - BB（Block Box）：每 10000 个区块生成区块盒子

◦YGGDRASH 区块同步速度

1 AKASHIC RECORD + 9 BLOCK BOX + 2 REGIONAL BLOCK SYNC TIME = 约 30 分

◦其它区块链区块同步速度

• BRA 适用结果

上述适用结果所示，BRA 是随着区块规模越大，越能将区块同步速度和节点资源最小化的技术。
同时可以积极的解决目前正在困扰区块链的区块规模问题，甚至可以将该技术
用于未来的 IoT 终端，
扩大区块链的实际应用范围。

2.2.4 通过文件共享网络（File sharing on P2P Network）解决存储容量问题

YGGDRASH 的文件共享网络记录有智能合约、阿卡西记录、区块盒子、链资源等。
APP 不只以编码的形式存在，而是和服务 APP 的各种形态的资源一起驱动。

YGGDRASH 通过文件共享网络为区块链上的数据限制提供自由，借此提供更多样、更丰富的区块链服务。

2.2.5 通过多维区块链保障相互运用性

YGGDRASH 之所以被称为多维区块链，就是因为区块生成时间可相互连接其它区块链。要理解区块链相互之间的连接，首先需了解区块链的时间概念。
比特币每 10 分钟生成一个区块，这就是比特币的时间。但以太坊和比特币不同区块生成时间是 15 秒。

那么，两个链之间又是如何连接的呢？YGGDRASH 在解决该问题上使用的是名为阿卡西切片（Akashic Slice）的链连接协议。在交换不同区块链上的数据时，会将节点的区块结果像照相一样储存下来。简单地举个例子，比如一个人正通过窗户观望窗外，假设一辆汽车正从窗外经过。那个人把汽车照了下来，这样就留下来汽车从窗外经过的证据。

如果其它区块链平台可以通过我们展示的链连接协议连接上干链的话，就可以使用我们的网络资源（YEED、信任度、其它 DApp）。这不仅可以解决监管的问题，就连现有的区块链平台只要连上 YGGDRASH 就能变成一个支链进行工作。

2.2.6 区块链启动&智能工具（Blockchain Starter&Smart Kit）

YGGDRASH 为独立区块链开发公司提供区块链开发模块。各模块是可根据自身商务需求和经营战略进行调整，具有快速性、灵活性、便利性等特点的区块链开发工具。

YGGDRASH 为致力与区块链技术发展的区块链开发工具，设置专属资金及开放资源环境。这是 YGGDRASH 计划中的孵化事业之一，将根据各参与者的贡献度给予相应奖励。

对区块链技术有兴趣或是想要为此贡献一份力量，无论是谁都可以参与进来。该技术可供任何人自由使用。

区块链开发工具由 2 种形态组成。

区块链基础设施开发工具将区块链的基本要素模块化，帮助区块链初学者更快、快高效地在区块链上展开自己的事业。

1. 区块链基础设施开发工具（Blockchain Starter Kit）
   - 协议演算（PoW、PoS、PoI 等）
   - 加密化演算（ECDSA、Hash 等）
   - 资料结构（Merkle tree, Patricia tree 等）
   - 节点/钱包构成（Full node, Light node, Web node 等）
   - 专业化功能（Smart Contract, Zero-Knowledge Proof 等）

区块链智能工具意在克服分片、闪电网络等区块链极限的新技术开发，并将区块链用于人工智能、物联网、遗传学等第四产业。YGGDRASH 不仅要营造出适合此类事业的环境，还希望能够和对区块链充满热情和能量的众参与者一同成为可以为人类做出重大贡献的先驱者。

2. 区块链智能工具（Blockchain Smart Kit）
   - 扩张性技术（Sidechain, Sharding, Lightning Network 等）
   - 相互运用性技术（Multidimensional Blockchain, Atomic swap 等）
   - 数据容量节俭技术（Akashic Record, Block Box, File sharing on P2P Network 等）
   - 第 4 次工业革命技术（Big Data 、IoT、AI、RT 等）

2.3 YGGDRASH 监管

2.3.1 协议演算

区块链的驱动是在不特定的多数 P2P 网络环境中进行的，因此就要解决“信息到达时差、系统操作不当和障碍，以及数据伪造”这些问题。

协议演算就是为了在上述环境中保证参与者能够到达单一结果，而在各节点对所建区块的正当性进行检验，并在整个互联网上进行共享。

比特币是最先通过名为 PoW（Proof of Work）的依靠计算量进行的协议演算，在 P2P 网络上实现了任何人都可以参与的电子货币系统。但是，由于区块链在结构上被分化，曾经使用短链的节点就被转为了长链，所以经常会出现账户余额出现变动，或是交易本身消失的事情。比特币为了避免出现此类现象，也存在设置了即使交易确定后不等 6 区块的话也不能进行交易的钱包。正是因为这种结果（数据完结性）的不确定性，成为金融机构很难导入比特币的原因之一。此外，为验证分散数据的其可信度，进行的复杂演算或多数节点协议时间也要比其它协议演算时间更长。这不仅很难提高处理性能（响应时间和处理量），更重要的是，其结构本身就不符合那些需要实时处理的业务。

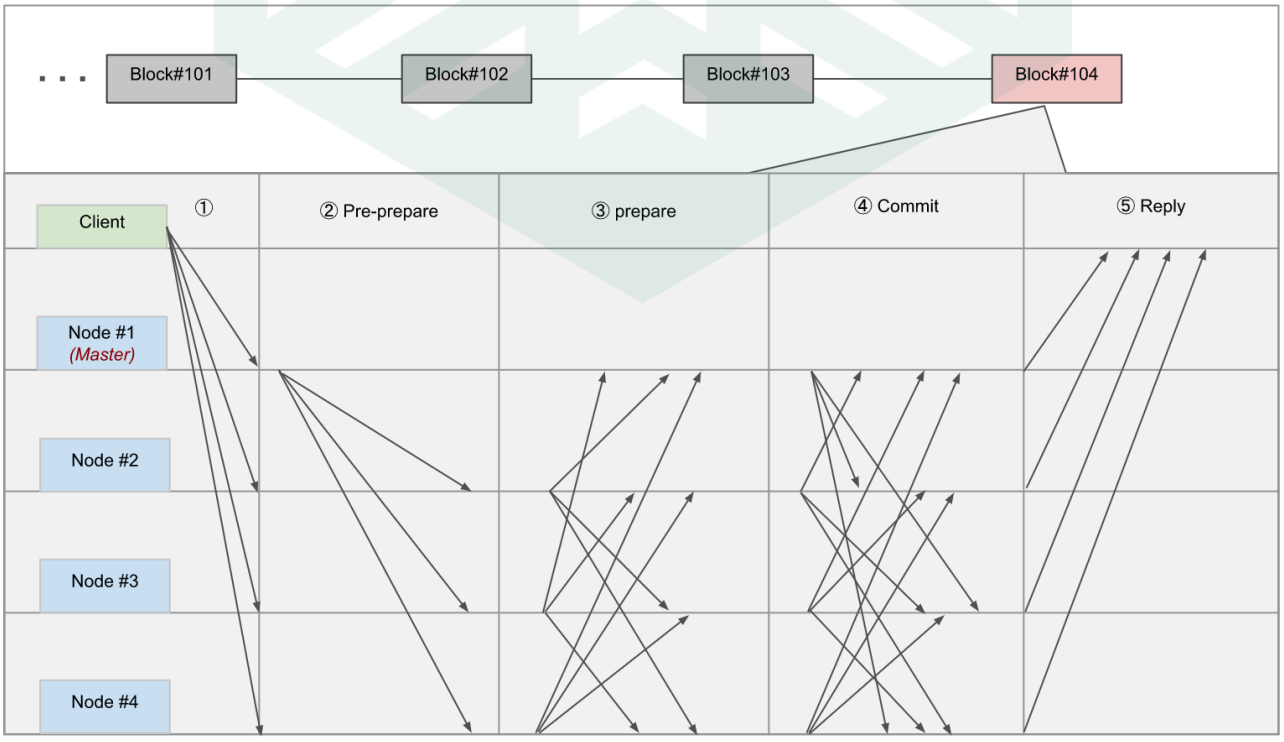
以太坊的情况使用的是 PoS（Proof of Stake），这种演算的特征是持有越多货币的节点优先生成区块。由此可以看出，其前提就是“拥有大量货币的节点为了保护货币价值，而不损失系统的可信度”。基本结构和 PoW 无异，只是因为会随货币规模的变化，降低散列难度，因此在节点的资源消费或处理速度方面比 PoW 更为先进。但是 PoW 和 PoS 都剩余的仍是解决结果不确定性和性能问题。

YGGDRASH 是基于 PBFT（Practical Byzantine Fault Tolerance）的 DPOA（Delegated Proof Of Authority）进行设计，可以改善 PoW 和 PoS 的结果与性能问题。

首先让我们来了解下 PBFT（Practical Byzantine Fault Tolerance）。

PBFT 是使节点的 1 名参与者成为主节点（Master Node），然后向区块发送包含自己在内的处理请求，在对请求结果进行汇总后，使用多数的值确定区块。
如果用 N 个表示不确定的节点数，节点数有 3N+1 个，确定时就需要 N+1 个以上的节点。

下面是 PBFT 的区块处理过程图示。



FBFT 处理过程

① 客户端向所有节点发送邀请

② 成为 Node#1（Master），按顺序将命令传给其它节点

③ 各节点接收到②的命令后，便会给包含 Node#1（Master）在内的所有节点回信

④ 各节点收到③传达的一定数量以上（2N）的命令后，便会给包含 Node#1（Master）在内的所有节点传送所接收信号

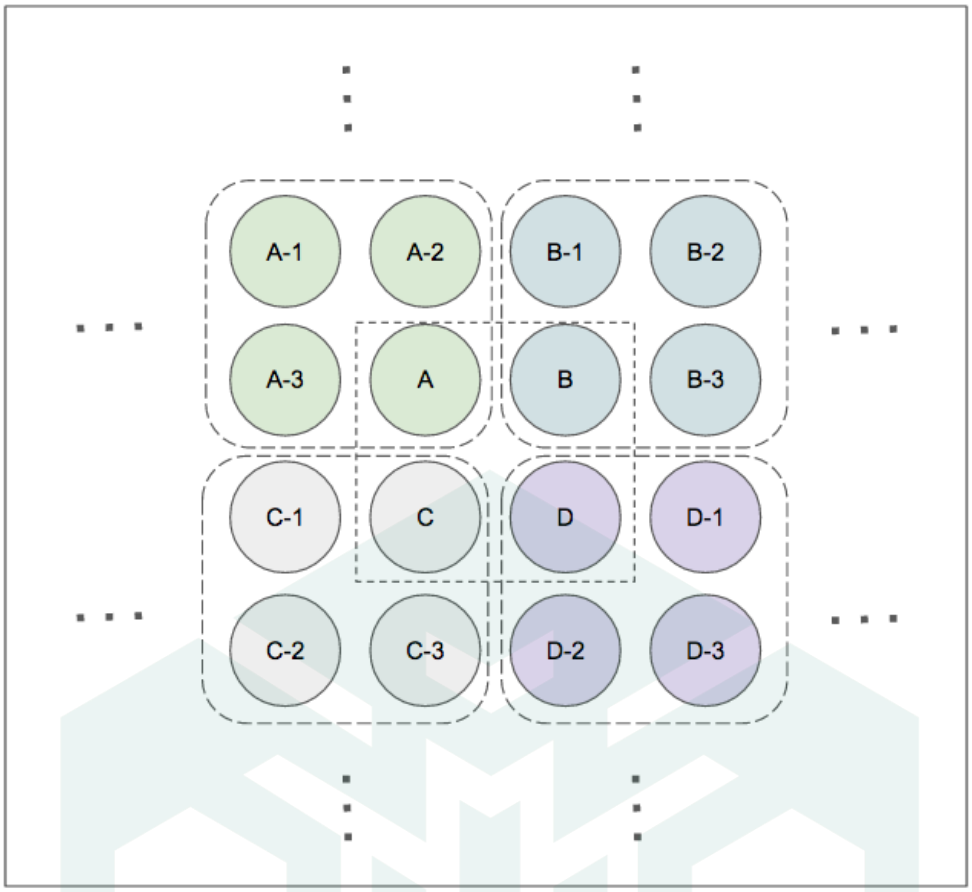
⑤ 各节点收到④发送的一定数量以上（2N）的命令后，便会执行命令，记录区块，把 Reply 向 Client 返还重放

与 PoW 或 PoS 不同，PBFT 是通过少数服从多数的原则进行决策后创建区块，因此不会产生区块链的分歧。换句话说，一经确定的区块就不会产生变动，结果也就可以得到保障。（是不会产生区块链分歧的结构）
此外，与 PoW 或 PoS 一样直到满足特定条件为止，演算不会反复进行，因此这是一种性能十分优秀的演算。

但是，PBFT 也有缺点。PoW、PoS 即使只剩下一个节点，依旧可以运行区块链。但 PBFT 只有满足一定数量以上的节点才可以运行区块链。换句话说，就是要解决主节点的单一失败点的问题。

YGGDRASH 设计为通过节点层次化（主节点&下级节点）解决该课题。基本区块检验是根据既定演算（Round robin 方式及时间序列方式），设计为每 10 秒生成一个区块。这个区块生成时间是通过测试四个过程调定的最佳时间。

各主节点设计为根据 YGGDRASH 权限委托政策将自己的代表权限委托给所属下级节点，在维持一定数量以上的节点的同时，对单一失败点进行改善（single point of failure）。



上述图示为 YGGDRASH 节点运行组成说明。节点中 A-D 字母表示主节点，而由字母-数字表示的节点是相应主节点的下级节点。节点的区块生成被制定完成后，会根据演算随机启动，当发生特定节点故障或延迟时，将启动权限转让过程，该启动的及时性，是应对故障的超强自检系统构造。
此外，如打算恶意使用节点权限，至少要先获取一半以上的权限。即使主节点说谎，只要所有参与者在监视主节点移动时判断其为不正当行为，就可以依照少数服从多数的原则替换主节点。
下面介绍 YGGDRASH 协议演算委托权限证明方式（DPOA：Delegated Proof Of Authority）。公共区块链应从基本无法信任的不特定多数节点中找出协议。比特币的“工作量基准”和以太坊的“押金担保”都是为了担保区块而设计的。
基本的区块链因其匿名性系统很难测定相应账户的可信度。
但是，YGGDRASH 账户使用的是和现实世界相似的可信度，可以建立网络或区块链上的或其它电子身份。

YGGDRASH 1）致力于在不可信的区块链世界建立一个可以积累信用的区块链世界。2）在 YGGDRASH 支链可信度评价链上会根据各节点的行为，对该信用进行增减。3）YGGDRASH 的主节点中长期贡献度最高的节点，即可信度最高的节点，在 YGGDRASH 网络，可通过主节点集团投票任命为信任度验证节点。4）这样，各主节点可获得 YGGDRASH 干链的“区块担保”和对 YGGDRASH 网络政策进行提案、改订和决定的最重要“权限”。

YGGDRASH 意在构建一个将不可信的环境打造成为值得信赖的环境，将只有追求眼前利益的参与者变为由追求长期利益参与者构成的生态区块链。

2.3.2 主节点的监管

主节点由 YGGDRASH 自身可信度评价链选出，3/4 主节点参与其中，只有获得一半以上的赞同，才能最终被任命为主节点。主节点集团可对 YGGDRASH 生态系统的运营政策、网络参与者的赏罚政策、YEED 的货币政策等进行投票和决定。此外，主节点的权限可根据“权限委托模型”对主节点进行委托、转让和退出。

YGGDRASH 的主节点以稳定性和安全性为基础，将由分散在世界各个大陆的主节点构成，主节点的个数会通过测试四过程选定一个最佳数字。

2.3.3 主节点的奖励机制

YGGDRASH 多维区块链的政策，是不能直接获取金钱报酬的构造。但是 YGGDRASH 的主节点可以获得不消耗名誉和 YEED 的永生链提案和免手续费等优惠。
YGGDRASH 主节点如出现未参与区块检测和政策等违反规定的行为，或是证据不明的恶意行为，可对主节点进行转让或终止，如恶意地实施不正当行为，则会被当退出。此外，如果代表者被投诉是否侵害节点，一经确认，相关代表者将被非活性化，对投诉人根据投诉政策给予一定比例的奖励。

2.3.4 YGGDRASH 货币（YEED）政策

YEED 作为 YGGDRASH 内部使用的货币，最初发行 100 亿个。至少 1 年的时间会出现 YEED 销毁，全体发行量会逐渐减少。YGGDRASH 会根据网络参与者的可信度交易手续费差别化，积累到一定程度信任度的账户，免除手续费。

YEED 的最大用途就是生成新的支链，并维持。YEED 的量决定支链的生命力，随着时间流逝，YEED 会逐渐被消耗。YGGDRASH 的生态系统不断发展壮大，YEED 的价值和 YGGDRASH 的干链、支链也会随之一同成长。可信度较低的账户所付手续费将用于 YGGDRASH 孵化预算，这将使 YGGDRASH 生态系统变得更加强大。

2.4 USE CASE

2.4.1 分散型交易所（DEX：Decentralized Exchange）

顾名思义，这就是“被分散的交易所”。在 DEX，货币的所有转入・出账都只在区块链上完成。也就是说，使用通过区块链直接连接的 YGGDRASH 个人钱包进行交易，而不是交易所提供的代币化内部钱包。分散化的交易所不能随意进行操纵行为，如任意阻拦转入・出账等；也不能实施恶意行为。这样做便可解决现有中央化交易所的货币黑客问题，以及个人信息泄漏问题。
YGGDRASH DEX 交易所将成为安全的去中央化交易所的规则改变者，有效改善现有中央集中式交易所的连接延迟、黑客风险、信任度等问题。

2.4.2 应用商店（DSB：DApp Store Of Blockchain）

YGGDRASH 的支链即是一个区块链，同时也是一个 DApp。从现有的以太坊来看，为运行名为 A 的 DApp，必须一起下载与此毫无关联的 B、C、D，这就出现了数据存储的非效率性问题。但，YGGDRASH 每个 DApp 区块链因为其服务的独立化，只需下载与特定 DApp 相关的支链即可。这就像用种子软件下载《星球大战》时，不需要下载种子软件中的所有电影。此外，YGGDRASH 作为多维区块链，还为所有 DApp 用户提供更容易更便利使用的类似于苹果应用商店一样的环境。各位脑海里出现了怎样的情景呢？各位想象出来的样子便是 YGGDRASH 的 DApp 商店。

2.4.3 未来景象

下面是我们想象的未来景象。

彼得有一个商务会议，他在自己的手机日程上记录了会议的地点和时间。为了前往会议场所，他走出建筑，在建筑前等待无人驾驶汽车。上车后，无人驾驶汽车便通过最佳路线向会议场所前进。行程结束后，彼得下车走进会议场所。

YGGDRASH 会对以上场景产生怎样的影响呢？记录会议日程的瞬间，安装在手机上的 YGGDRASH 便会立刻呼叫最近的无人驾驶汽车。距离最近、评价最好的无人驾驶汽车在接收命令后，立刻到达目的地，等候彼得。彼得乘车的那一刻，就显示出了费用，在到达目的地后便会自动扣费。扣费成功时，无人驾驶汽车的评价就会提高，根据无人驾驶汽车持有支链的代币数量，按照一定比例收益自动分配。即，想要投资无人驾驶汽车的人只要买入特定无人驾驶汽车支链的代币即可完成投资。

如果彼得没有出现，就会给彼得的评价减分，对彼得产生无人驾驶汽车使用费提高或增加等待时间等不利的影响 。

3. YGGDRASH 核心及结论

3.1 What kind of, Discriminate, Blockchain? （何种，有差别的，区块链？）

YGGDRASH 的核心原理是承认 1）分散化导致处理速度缓慢（必然比中央化系统相对缓慢）；2）只得依靠不特定的多数检验节点维持区块链网络的经济奖励问题；3）持续增加的区块链容量和区块同步速度问题，为上述问题提供最现实、最易实现的解决方法。

3.1.1 各区块链的独立性和处理性能保障

1) 主链处理性能最优化

YGGDRASH 的干链是连接所有支链的通道，通过以下方法实现处理性能/容量的最优化。

- 区块数据大小轻量化

干链保有的数据只是各支链地址信息等最小程度的信息，将数据体积最小化，随时间流逝，可减缓数据大小呈线性增加的问题。

- 优化区块生成的协议流程及方法

我们使用 OPOA（Delegated Proof Of Authority）协议演算。本协议演算以稳定性・信任性为基础而设计，优化协议流程/演算/时间的最小化及协议参与者数，提高处理速度。

2) 各区块链（DApp）独立的网络，监管保障

各个区块链都不隶属于上级链，而是应该拥有独立的区块链网络、监管、数据、货币、服务等。不应保留自身不需要的其他区块链（DApp）数据，及维持此类数据而使用资源。此外，其它链发生交易延迟时，不能使其影响到自己的服务和网络。

我们引入了干链和支链这两个概念，解决了该问题。简单来说，就是根据各区块链服务的特性和目的，组成各自不同的区块链，这样一般用户使用区块链上的 DApp 时，就可获得无延迟的服务。通过这种方法，打造一个由真正意义上的 DApp 构成的环境可服务生态系统。

3) 为 YGGDRASH 网络参与者提供多样的区块链技术・服务工具

YGGDRASH 为各支链的处理性能及区块链商务用户提供多样的技术服务。

- 通过区块链网络分片（sharding）提高处理性能
- 通过 BRA（Block Reassembling Algorithm）提高节点同步速度
- 通过文件共享网络（File sharing on P2P Network）提升数据存储性
- 提高智能合约数据存储性
- 通过区块链启动&智能工具（Blockchain Starter & Smart Kit）提高区块链服务的便利性・效率性

3.1.2 解决利己性的挖掘竞争及保障基于信任的经济奖励

1) 解决利己性的挖掘竞争体系

公共区块链上负责区块协议的节点（=挖掘者）是维持区块链的最重要的因素。但是，随着需处理的交易增多，节点（=挖掘者）为保障高手续费的交易，就会出现利己性的竞争。

YGGDRASH 通过 DPOA 可以解决利己性挖掘竞争问题。与 PoW、PoS 使用加密货币获取奖励不同，YGGDRASH 区块链检验者拥有决定 YGGDRASH 网络政策的权限。因此，YGGDRASH 区块检验者不会为获取经济奖励而实施利己性挖掘，这样就可以建设更加健康及庞大的 YGGDRASH 网络。

2) 基于信任的经济奖励保障

YGGDRASH 拥有单独评价各支链和用户信任度的支链（信任度支链）。该支链设计为对任何人以公平的“时间”资源为基础对信任度进行评测，惩罚恶意用户，同时保障给予善意用户免除手续费等经济性奖励。

3.1.3 区块链间相互联通・扩张性保障

根据各区块链的商务需求，YGGDRASH 作为与其它区块链连接的区块链平台，干链和支链担当连接的角色。和在谷歌搜索时使用的域名服务相似，干链保存有与 YGGDRASH 网络相连的所有支链信息。支链可选择干链保存的各个支链信息中自身商务需要的服务进行连接。

上述说明的各区块链的独立性、经济性奖励保障，及与其它区块链商务相连时，才是真正意义上自由竞争市场的开端。

初期，各区块链应只建立自己的区块链和服务，将重点放在时间上。以后，各区块链就会发现我们 YGGDRASH 的其它优秀区块链服务，通过相互连接，体验制作其它形态的商务模型。这种融复合服务越多，我们的网络就会越丰富，使用该服务的用户就会流连于我们的区块链生态体系。

3.2 What kind of, Incentive, TO ME？（对我来说，何种，奖励？）

YGGDRASH 设计为所有区块链生态系统参与者都可获得经济奖励。我们的目标是建立不是财富和权利拥有者可以垄断的区块链生态体系，而是一个对所有网络参与者来说都是透明、公正且合理的生态系统。

3.2.1 加密货币开发者

不考虑其它区块链交易延迟问题，根据自身商务日程可开发和提供服务。以往为了进行原子互换，在与其它链连接时，需要开发资源。而现在，只需依照自身商务战略连接各支链，即可享受 YGGDRASH 提供的各种区块链技术。

3.2.2 加密货币挖掘者

支链挖掘者：以 YGGDRASH 提供的链信任度信息为基础，选择可信任的链，保障挖掘者的稳定挖掘收益。
YGGDRASH 全体：对包含支链在内的整体 YGGDRASH 链来说，依靠众多挖掘者，可建立稳定的网络生态体系。

3.2.3 加密货币使用者（投资者或服务用户）

以 YGGDRASH 提供的链信任度信息为基础，选择可信任的支链，为投资者提供稳定的投资率，为服务用户提供稳定的服务环境。此外，信任度高的用户还可获得免手续费等附加优惠。

3.2.4 加密货币服务供给者

利用 YGGDRASH 提供的区块链启动&智能工具（Blockchain Starter&Smart Kit），快速且高效地完成自己的服务，同时连接与 YGGDRASH 相连的丰富区块链服务，建立可持续发展的多种融复合服务。

3.2.5 加密货币交易所

利用 YGGDRASH 信任评价信息，可提前预防因特定链（货币）问题导致的交易所・交易所用户的损失。此外，获取规格化的钱包模式，可将货币上市等所需开发资源降到最小，同时，将符合交易所自身货币上市/运营等商务战略的交易所收益极大化。

E-Mail : info@yggdrash.io

Homepage : https://yggdrash.io