ValueCyber 白皮书

下一代兼具弹性的区块链数字经济系统

目　录

一、背景

区块链技术在近期的迅速发展已经无需我们过多地进程阐述。当前以以太坊为代表的区块链技术的核心特点之一是图灵完备能力的“智能合约”，允许开发者基于一个底层框架（通常是以某种虚拟机的形式）自由地构建任意应用，并通过区块链以去中心化的形式运行。

这一模式虽然使以太坊理论上具备无限的扩展性和可能性，但在现实中，以太坊能达到的能力边界，亦即其所执行的智能合约能完成的工作，是很有限的。这种限制的来源是区块链的另一个本质属性——共识机制。区块链作为一个去中心化同时又具备一致性的系统，必须为这一实现付出相应的代价。这些代价包括：

- 信息传递和同步
- 历史的记录和验证
- 在非互信的个体之间实现协作

在对区块链的研究和理解过程中，我们认识到上述代价可能具备重要的意义。本质上，这些代价实际是去中心化的本质因素，因此是区块链系统中必须的组成部分；同时，它们又构成了区块链系统的能力边界，并随着去中心化程度的增加而增加。例如，信息传递的延迟将影响系统的共识能力（如降低 POW 共识机制算力攻击的 51%上界）；而记录和验证历史（区块）的需求将使得区块链中存储和运算能力较低的节点消失，系统逐步失去其去中心化特性。

以太坊提供的近乎无限制智能合约的能力实际上激化了历史记

录和验证的代价对系统运行的冲击。一方面由于任何合约都必须被全体节点所执行，一个应用不可能无限制地扩展；另一方面众多的应用在同一个区块链上执行，在实现上是一个巨大的挑战（2016 年以太坊遭受的 DDOS 攻击便是一个典型的例子[1]），而系统资源的有效调度更是几无可能。以太坊的区块数据量迅速增大，当前已经大大超过了比特币。但当我们从代价的方向来审视时，容易发现以太坊的实现形式是相当浪费的：考虑以太坊上不同的应用存在着不同的用户群体，然而特定应用的用户却需要为其不感兴趣的应用承担相关历史记录和验证的开销[2]。

过高的共识代价带来的后果是区块链中用户和“共识者”（即记账者、“矿工”）群体的分离：用户仅仅是利用区块链而不再参与系统的运行，只是简单地通过支付一些代价而将系统完全交到共识者手中。我们并不打算在此深入讨论这两个群体之间的关系，但我们认为这样的关系形式已经偏离了区块链作为“去中心化的协作工具”的初衷，并实际上产生了某种程度的中心化。这并不仅仅是某种共识机制（如 POW）所带来的问题，而是区块链本身实现共识的需要带来的问题。由于前述的各种代价的存在，即使将共识机制从 POW 转换到 POS 也并不能彻底解决这一困难。

当展望区块链的未来时，我们期望下一代的区块链将能够回归其作为新的协作方式的本质，区块链的使用者同时也是系统运行责任的

[1] https://news.ycombinator.com/item?id=12557372

[2] 诚然，以太坊允许用户只下载其需要的部分的区块数据；然而这一点并不适用于矿工，亦即区块链系统中真正承担共识代价的成员。

承担者，因而获得真正意义上的去中心化。为此我们必须正视共识代价问题并加以解决。我们主要的观点是：

- 区块链是某个**共同体**为了实现某种**协作**而使用的**工具**；
- 信息的同步，历史的记录和验证不需超出共同体的范围，并以满足协作所需为限；
- 共同体概念是可以蕴涵的（亦即存在“共同体的共同体”），互信和协作的实现存在于共同体之内，也存在于共同体之间；

我们由上述观点所推论的未来区块链使用场景和 Gavin Wood 等的构想相当一致[3]，即一个存在众多区块链的世界，每个区块链独立地为一个共同体提供某种协作的实现，而不是一个可以承载一切的巨型区块链[4]。不同的区块链可以托管其一致性（类似于 Polkadot 中的 pooled security 概念）[5]，并通过某种方式和其它区块链相互作用，从而实现共同体之间的相互协作。

为了实现这一未来的区块链技术图景，我们和其它持相同观念的研究者一样在一致性聚合，链外和跨链协作等方面进行了探索。ValueCyber 是这些探索得到的产物，我们期望它能成为下一代区块链技术图景中的一个有意义的范本。

[3] Gavin Wood, *POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK*, https://github.com/w3f/polkadot-white-paper/raw/master/PolkaDotPaper.pdf

[4] 这并不意味着以太坊这样的系统没有存在的意义。相反，以太坊迅速地为一个共同体建立协作的能力是无与伦比的；但是当共同体的协作活动期望更高效和稳定地进行的时候，采用独立的区块链将是更好的选择。

[5] 注意一致性的托管和用户-共识者（矿工）的分离是不同的；前者中用户共同体仅仅是将其历史的一致性问题交托给第三方（如 polkadot）处理，从而使历史获得更高级别的确定性；但是并没有放弃历史的记录和验证责任。

二、ValueCyber 项目概述

ValueCyber 是面向数字经济时代的生产和流通所需的协作而设计的区块链系统，也是一个尝试实现下一代区块链的技术和开放性需求的区块链。在 ValueCyber 的实现中，我们重新审视了区块链概念，并尝试扩展当前区块链的实现边界。进而实现高灵活性的区块链经济自动化平台。ValueCyber 期望解决的需求是生产过程中的流动性，为了实现这一点，ValueCyber 不仅支持一般加密数字货币的流通符号功能，更将其支持的流通协作范围扩展到了债务领域。

ValueCyber 的核心思想来自于对当前区块链实现的重新审视：区块链是一个基于特定规则来处理外部输入（事务）并生成特定的历史（区块）的系统。因此，区块链系统的创造者必须在系统运行之前，就考虑到几乎所有可能的输入的模式并实现相应的处理规则。一旦处理规则需要变动，则要求整个区块链系统对此变动取得共识，随后通过系统升级、链分叉等一系列漫长的路径实现。

当考虑引入债务这一概念时，我们发现其难以使用一个确定性的系统进行处理。例如我们应当如何判断哪一个用户有能力负担，以及可能负担的债务数量？这并不是一个可以通过（区块链的）历史和简单的处理规则就解决的问题，并且很可能是一个随着应用环境和时间而不断改变的问题。因此即使我们通过庞大的输入参数和复杂的处理逻辑去为系统中的用户表达债务，这些规则也很可能由于环境的变化和时间流逝而失效。而一旦生效，系统又需要为共识新的规则付出巨大的代价。简而言之，一个确定性的区块链系统不足以提供足够的灵

活性去支持类似于债务这种复杂和多变的事务。

因此，这要求我们设想一种可能，即复杂事务的分配不依赖于任何预先设置的规则，而是在系统运行时被随机应变（亦即 case by case)地决定。在区块链的话语体系中，通常会引入一个神谕(oracle)模型被用于实现上述需求。但这意味着一个必须被信任的第三方的存在，区块链的历史实际是被 oracle 所控制，这样的系统已经脱离了区块链系统的去中心化特征。

这是一个两难的问题：将历史的产生（事务的处理）从确定性中移除赋予系统最大的灵活性，然而这样的系统不再是一个能通过共同体内部基于区块链的协作就独立地运行的系统，因此实际上损失了去中心化。但是，如果我们意识到协作的共同体的能力并不仅限于处理历史，上述的两难就可以被解决了。解决的关键在于设置规则允许神谕机并不一定被每个成员所服从。这在区块链系统中，最常见的方法就是事务过滤，亦即拒绝神谕机的命令。在共同体广泛地执行事务过滤的情况下，系统整体就实现了从听命于神谕机到对抗神谕机的转变。而这一改变的程度取决于共同体内部共识的广泛程度。

基于上述设想所得到的系统是一个扩展了区块链系统外延的产物。在对此的探索中，我们总结出上述系统应当符合的前提条件如下：

1. 系统引入的神谕机在多数情况下是可靠的第三方，其行为和系统本身的利益一致；

2. 神谕机不能在单个 case 中显式地损害协作共同体特定成员的利益（防止多数暴政）；

3. 神谕机不能在单个 case 中**显著地**损害系统的整体利益，亦即在神谕机对系统产生危害的情况下，危害是渐进的，并且在一定范围内是可容忍的。

4. 协作共同体有能力识别神谕机作出的损害系统整体利益的行为，并在**有限时间**内达成共识，最终阻止神谕机的危害行为[6]。

5. 神谕机无法在协作共同体达成共识的时间内对系统产生显著的危害

由此获得的非确定性事务处理的能力是 ValueCyber 最为创新的特征：在引入神谕机（在 ValueCyber 中称为特权组）对债务相关事务进行管理的情况下，保持系统整体的去中心化。由于特权组的存在，ValueCyber 无需事先为债务管理设置相应的规则，系统以非确定性的形式运行（同样的债务事务输入可以得到完全不同的处理结果）。同时，通过确定性的机制，ValueCyber 的用户可以阻止特权组对系统作出不利的举动；并且即使特权组的行动被完全阻止，系统整体仍然可以保持大部分的功能。

最后，ValueCyber 作为下一代区块链的技术的范本，在一致性共享和协作能力上也作出了自己独特的尝试。我们独立地提出了一种类似于比特币的 schorr 签名方案的集体签名机制，允许外部的共同体和单个用户一样应用 ValueCyber 提供的流通支持能力；ValueCyber 自身的共识机制设计也考虑了一致性托管的可能性，并包含一个和比特币区块链共享一致性的实现。

三、ValueCyber 的技术架构

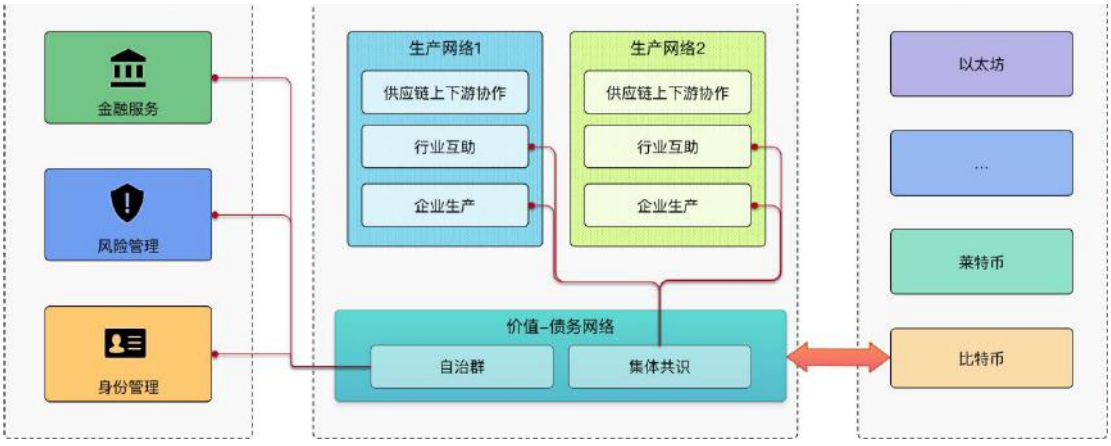
我们的最终目标是实现一个为现代以及未来的社会经济自动化服务的区块链平台，致力于解决下列两个问题：

1. 商品生产过程中的流动性
2. 商品生产过程各环节之间和环节中多个生产者之间的协作

流动性问题是每个生产者最可能遭遇的噩梦。即使市场一帆风顺，生产运作一切正常，某个环节中账款的拖欠仍然可能导致整个企业的资金链断裂乃至破产。ValueCyber 的设计目的即是要解决企业生产过程中对流动性的需求，并通过协作实现同业互助和产业链互助，帮助生产者抵抗产业和市场中的波动。

3.1 生态体系

严格来说，这一蓝图并不仅限于 ValueCyber 本身，而是以 ValueCyber 作为流动性支持的基础，如下图所示的架构：



基于一般等价物的价值交换是社会生产和经济活动的基础。对应地，ValueCyber 是以加密数字货币（比特币）为原型的区块链系统，我们也将其称为“价值-债务网络”。ValueCyber 作为实现生产者主体之间和生产环节之间的资源交换和价值流通的基础工具，具备超越

传统的加密数字货币的去中心化特性，亦即系统真正地由参与者共同维护和运行。因此，每个参与流通活动的个体（用户）同时也可以是ValueCyber 运作的参与者。此外，价值-债务网络具备对现实世界的开放性，允许外部组织和系统的相互协作。例如，债务的准入机制由外部的身份管理组织实现，为网络中的主体（账户）提供了身份唯一性保证，进而实现责任机制。因此，价值-债务网络中可以实施超越比特币等数字货币系统能力的经济活动。

ValueCyber 的价值-债务网络在实际运行中允许实名（经过准入系统验证）账户和匿名账户并存。但是匿名账户的能力被限制在仅能进行现金流通相关范围的事务。一般地，实名账户在 ValueCyber 中代表的是单个生产者或经营主体，亦即工作室、工厂或企业；个人则可以通过无门槛的匿名账户参与价值流通过程。

ValueCyber 系统支持生产者基于区块链技术实现资产的数字化、确权、信息流通和资源交换等生产特别是数字经济时代数字化社会大生产中的商品生产中必不可少的各种信息活动。但是和当前许多区块链给出的大而全的实现方案不同，各种生产信息活动被设计由多个相互独立的区块链承担，并构成生产网络。生产网络的参与者可以是企业内部的多个部门或集团，也可以是供应链上下游多个环节、或者同一商品生产/同一行业中多个生产者构成的行会。其中每个区块链独立地维护其历史和运行，链内的各个参与者基于区块链技术实现高效的信息共享、生产资料流通和行业内互助等各种可能的事务。而价值-债务网络作为生产网络的底层支撑，仅负责实现各个区块链之间的资源和价值交换，以及和其它区块链系统之间的价值交换。

如前所述，区块链是一种参与者在共识事实的基础上进行协作的系统。参与者（节点）的数量越多，共识的范围越广泛，系统的可靠性和公信力就越强；然而另一方面，要在越多的参与者之间实现共识，困难和系统的开销就越大，在单位时间内可以达成共识的事实数量越少。这是限制比特币等匿名节点的加密货币系统的事务处理规模的根本因素。社会生产活动将产生海量的信息，一个区块链系统要同步和共识这样规模的数据，即使在共识机制上有所改进，也仍然无法支持如此巨量的事务量，同时还不牺牲开放的区块链所具备的可靠性和可信性。

因此，价值-债务网络本身被设计为仅支持单一的“价值交换”概念，将共识的内容限制到一个很小的范围内，从而换取更为广泛的参与者规模。不同的生产过程的协作所需的信息和历史局限到实际参与对应过程的共同体之内，构成多个独立的生产网络。这一模式和现实世界中的生产模式是高度对应的。

因此，我们构想的蓝图整体是以 ValueCyber 的价值-债务网络为基础，符合下一代区块链技术图景的多个区块链的集合体。除了 ValueCyber，我们也将为生产者提供构建区块链的方案、部署和运行上的技术支撑，例如区块一致性的托管，以及区块链间交易等允许独立区块链有效工作和彼此联系的关键技术；并为经济活动构建需要的信息交换平台。所有这些区块链通过开放的功能入口和协议实现协作，而并不仅仅是简单地将公众链+联盟链拼凑在一起的体系。

ValueCyber 价值-债务网络对其它协作共同体（包括基于区块链的协作共同体和其它形式的协作共同体）开放的功能核心是我们实现的独创性的新型事务：集体共识事务。这一事务允许价值-债务网络内复数个账户构成一个集体，并以集体意志在价值-债务网络内执行相应的价值（数字货币）的转移。也就是说，不同于当前的数字货币系统在每个事务中只能验证单个或有限个账户的许可，ValueCyber 的价值-债务网络节点有能力识别任意数量的账户构成的集体所发出的许可并执行相应的事务。这是 ValueCyber 系统所独有的技术能力之一。

本白皮书后续的章节将按如下方式组织：我们首先阐述ValueCyber的基础即准入系统和主体价值-债务网络的技术实现；然后论述基于价值-债务网络的工业生产流通模式；最后我们将介绍ValueCyber为生产链提供的技术支持细节。

3.2 准入系统

在现代的生产和经济活动中，“负债”是和资产几乎具有同等重要作用的概念。两者共同构成了现代金融系统的基础。因此，ValueCyber的设计目的之一是解决这样一个问题：

一个区块链系统是否可能像其表达数字货币一样表达数字化的负债（Liability）？

我们认为一个完全基于匿名账户的系统是难以实现这一点的。负债的履行要求某种强制力存在。对于一个独立系统而言，这种强制力必须被扩展到系统之外，否则一个账户总可以以脱离此系统的方式摆脱其应履行的义务。（除非“脱离系统”本身对账户来说就是无法接受的，例如一个自然人不太可能通过脱离整个人类社会的形式去逃避其身上的债务。）孤立的匿名数字货币系统即使通过预先担保等方式来引入负债概念，其本质上仍然只能是某种现金交换的变形，这些概念上的“债务”所对应的现金会对系统流动性造成相同的影响，而不能真正像现代金融体系一样通过负债来平衡生产规模和流动性。

为此，ValueCyber 引入了准入系统的概念。准入系统为ValueCyber 和真实的社会活动之间建立关联，从而允许在

ValueCyber 中某个账户行为的影响扩散到系统之外。这使得 ValueCyber 的价值-债务网络不仅具备常规的加密数字货币功能，还能运行以负债概念为核心的更多类型的经济活动。

准入系统的命名来自于 ValueCyber 最初的构思，即一个负责审查用户执行债务事务资格的系统。而在当前的实现中，准入系统已经扩展成包括用户身份验证，担保和债务能力评估，风险控制和债务追偿等所有和债务事务相关而不包含在 ValueCyber 实现内部的所有任务的执行者总体。价值-债务网络允许任何的匿名账户在其中运行和数字货币相关的确定性的事务（transaction），但仅允许通过准入系统来运行和负债概念相关的非确定性的事务。一般地，准入系统首先将允许执行债务事务的账户限制在一个范围之内：这些账户在 ValueCyber 中为负债履行的义务不仅存在于 ValueCyber 系统内部，还会扩展到真实社会之中。亦即这些账户在真实社会中具备可追溯的实体，因此是通常意义上的“实名”账户。准入系统负责维护特定的账户和其在现实社会中的对应关系。

ValueCyber 的目标在于服务工业生产系统，其账户概念天然地与生产主体相对应。在 ValueCyber 中，实名账户通常对应于工厂、生产企业和公司等法人团体。使用实名账户的个体（法人团体）一般不需要匿名性，且更易于将其在 ValueCyber 系统内的责任扩展到现实社会。

准入系统在价值-债务网络中表现为一个自治的账户（公钥）群，群成员本身的增减可以通过群内已有成员的共识决定。ValueCyber 将“基础自治群”的概念应用于所有这种作为系统运行要素之一并且进行自治管理的团体，准入系统是价值-债务网络中的第一个和当前唯

一的基础自治群。

准入系统通过在价值-债务网络区块链上发布特定形式的事务来更新准入系统当前的成员。这些事务允许（所有的“基础自治群”概念都具备相同形式的事务）：

- 增加一名成员（公钥），事务要求自治群内所有成员一致承认；
- 删除一名成员（公钥），事务要求自治群内所有成员（除被删除的成员外）一致承认；
- 更新一名成员（公钥），事务要求自治群内所有成员包括将被更新的成员的一致承认；

一个基础自治群在实现中是定义在 ValueCyber 节点中一个或多个被信任的元祖账户（公钥），因此节点将接受元祖公钥随后发布的事务并更新此自治群在节点本身所记录的列表。按照我们的设计，准入系统最初将由 ValueCyber 运营方维护。为了保证系统安全性，元祖公钥将在创世块之后建立额外的 2 个公钥，使准入系统最少包含 3 个公钥并分别保存其私钥。

由于准入系统的存在，ValueCyber 可以以非确定性的方式处理债务的生成和分配到账户。进一步，ValueCyber 通过引入信用的概念将特权组的债务分配行为显式化。在系统中，信用 =（未来某时刻）等价的现金 + 债务（更具体的阐述可参考“基于价值-债务网络的经济表达”一节）。债务的分配是由准入系统向特定用户分发信用来实现。因此，特权组分发的信用总量 = 系统未来某时刻可能存在的现金最大值（如果所有的债务都没有偿还）。在规定时间内未偿还的债务将变成坏账，相应的用户在系统内的行为将被冻结（并受到惩罚）。

准入系统对系统中存在的坏账负责。

信用的引入实现了 ValueCyber 用户共同体和准入系统之间的协作过程：准入系统通过提交发放信用的事务向系统中加入债务，用户共同体则可以通过监测债务和坏账总量评估准入系统工作的质量和是否存在恶意行为，并通过拒绝信用事务的方式约束准入系统的行为。由此构成的系统符合我们在第一章中描述的系统的特征，我们可以总结出和前述系统特征相应的对应关系：

1. 是显然的（准入系统的正常行为符合系统利益）。在正常的情况下，准入系统对其发放的每一笔信用负责，并有效地控制系统的债务量和坏账率，通过调节债务的分配使系统内部的流动性更加高效；由于信用的发放经过有效审核，债务总是被正常地偿还，系统整体的现金数量仅在一个小范围内波动而不会显著地影响币值；在长期范围内，用户共同体还可以基于共识去实现各种可能的经济策略[7]；

2. 在系统内，用户任何的债务都必须被偿还。因此准入系统并不能在系统内显式地使特定用户获取利益，或者损害特定用户的利益；

3. 准入系统对系统可能的危害行为取决于坏账的总量，少量的坏账并不会显著影响系统的利益，并且准入系统在正常情况下将对此负责；

4. ValueCyber 用户通过计算系统当前的负债率和坏账率即可明确地判断准入系统是否对系统造成危害，并通过阻止准入系统的信

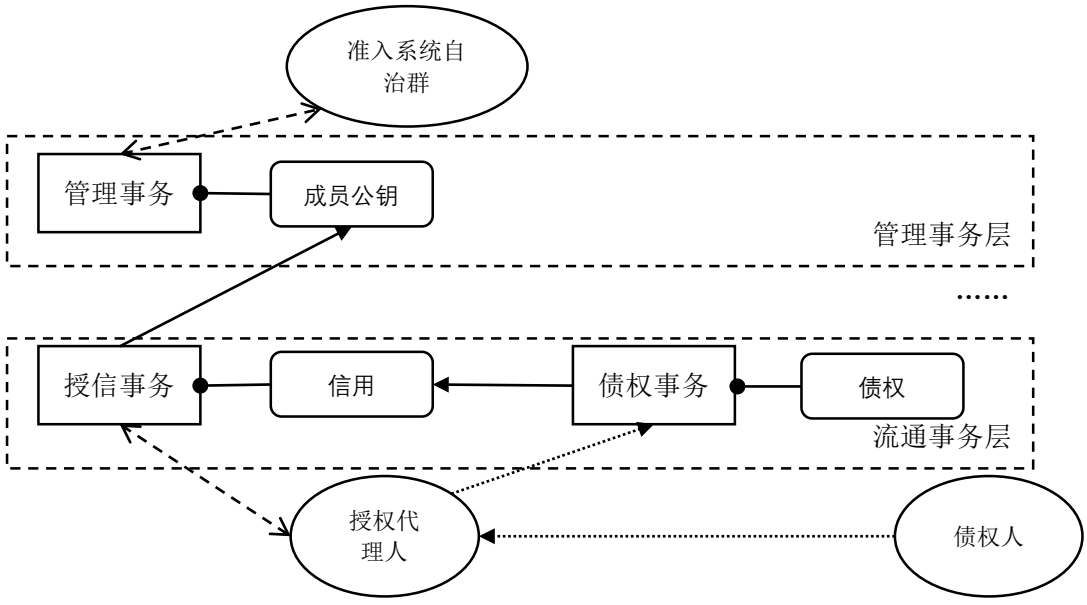
[7] 例如，在一定时间内加速币值的贬值；对照世界上国家的货币政策，这并非是不可能的

用发放阻止系统内现金总量持续的恶性增长；

5. 通过控制准入系统的信用的发放速度即可相应地限制现金总量的增长速度，亦即准入系统在作恶的情况下系统受到危害的程度；

通过信用概念，价值-债务网络可以将其它债务活动相关的信息和历史（例如实名认证信息，用户信用，风险控制数据等等）移动到系统以外。系统不需为这部分内容实现共识，这符合了我们对下一代区块链的描述：仅对最必要的要素进行共识，以最经济的方式去支付系统共识的代价。轻量化的共识代价是允许价值-债务网络能被最广泛地参与的基础。

可见，包含了准入系统的 ValueCyber 价值-债务网络是一个被真正实现的，超越当前区块链概念的系统，结合我们设计的”非确定性共识“机制，这一概念系统的实现合理性和细节将在共识机制和经济表达章节中进一步阐述。在实际运行中，准入系统的基础自治群并不一定直接面向用户进行信用的发放，而是通过一层额外的代理来实现，如下图所示。因此在准入系统中构成了一个自顶而下治理的金字塔式结构。



为更为有效地支持准入系统的实际运作，我们为 ValueCyber 准备了一系列相关的技术方案。例如，为了在区块链历史数据中有效地识别实名账户要求特定的公钥被登记到准入系统中。一般的公私钥方案（比特币的原始方案）将无法具备匿名账户可以自由更改其事务公钥的灵活性和安全性。因此基于 BIP-32[8]的继承式确定性（Hierarchical Deterministic）公私钥系统将被准入系统强制应用于实名账户。已经被认证的实名账户可以使用其主公钥或子公钥签发其事务。对 HD 钱包的支持和可表达账户密钥节点树的地址格式被加入到 ValueCyber 节点的实现。

由准入系统实现的非确定性债务事务处理为 ValueCyber 的债务表达提供了巨大的灵活性。但是一个完全独立的准入系统并不是 ValueCyber 所期望的最终形态。ValueCyber 最终应当能以基于本身的运行历史，结合量化模型和人工智能等方案，对所有账户实现有效的风险评估并设定责任（债务）上限，同时基于本身的规模所产生的用户粘性，从而逐步摆脱对独立的准入系统的依赖。在这种情况下，准入系统的运作实际是由 ValueCyber 的用户或部分用户构成的另一个合作共同体（很可能基于另一个区块链），整个系统在一个更高的层面（协作共同体的共同体）上实现自洽的，准确定性的运行。我们将此设定为远期研发目标之一。

[8] https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

3.3 价值-债务网络

ValueCyber的价值-债务网络是一个基于区块链表达的分布式账本的协作系统，也是 ValueCyber 系统中和比特币最为类似的部分。本节将比较价值-债务网络的实现和比特币的异同，并具体阐述价值-债务网络中创新的实现部分。

- **为什么是比特币**

比特币事务所使用的 UTXO 模型允许相对简单的历史验证过程，即对于特定的事务，我们可以通过简短的信息给出其在区块链上的的存在证明，而不需要验证者具备对整个历史（全部区块）的知识，因此适合于 ValueCyber 追求共识效率的特点。我们在 ValueCyber 的实现中花费可观的工作量，来保持整个系统的 UTXO 特性。

从可靠性考虑，比特币是第一个也是目前被最广泛应用的数字货币实现，其可行性和安全性已经得到长期的验证，而比特币在发展过程中的曲折和所积累的经验也是后继者最佳的参考。在 ValueCyber 系统中，价值流通是系统运行的核心内容之一，同时也将是最广泛的应用。这和比特币的设计目标是一致的。以比特币的协议和实现为基础，是目前最稳妥和有效的方案。这样一个相对成熟的主体平台可以允许 ValueCyber 团队后续将更多的力量放在生产网络相关的研发上，为工业生产提供更有效的技术支撑。

最后，ValueCyber 通过保留一部分比特币的实现和通讯协议，实现了和比特币的共享一致性能力，借助当前世界上可以得到的最大的算力机器的保障，ValueCyber 得以实现更为有效的共识机制。

3.3.1 配置共识和历史共识

区块链是一个所有参与节点具有共识的系统。在任何区块链实现中，存在一个显然的共识即“当前头部区块的标识”（通常是头部区块的哈希值），用于标识一个独一无二的区块链历史；然而，区块链系统实际还存在一个隐式的共识即”协议“的共识。正是后者确定了

一个节点应如何从头部区块的标识开始获取和验证整个区块链的历史，以及如何和其它节点协作。以比特币为例，后者共识的一致是通过比特币社区发布新的改进协议（BIP）和相应的实现（例如BitcoinCore）来取得的。但是比特币的实现中缺乏明确地表达协议共识的机制，由此带来一系列的问题：

- 没有显式地表达参与者对选择协议（投票）的机制，只能通过重用区块版本号的方式（BIP09/34），灵活性受到限制。例如 BIP34 的方案无法同时对多个方案并行地投票和选择，后续 BIP9 虽然改进了这一点，但仍然不易表达存在互斥关系多个方案9；
- 由于 BIP9 的应用，实现上已经无法从单个比特币区块的内容判断一个 fork 是否被应用，而必须通过整个比特币的历史来确认这一点。而且使得实现难以识别发生硬分叉（hard fork)后的数据，这可能为硬分叉后的 SPV 实现带来隐患10。我们认为 BIP9 实际上导致硬分叉过程的执行变得更加困难；
- 所有 BIP 的表达和部署过程都被固化在比特币的实现代码内部，导致比特币社区意志的实现高度依赖于开发者。在代码发行版本增加的情况下，任何改动的实现不仅要求社区成员的共识，还要求开发者开发进度的一致（或迫使部分用户重新选择其它发行版本）。此外，新代码版本的发布和重新

[9] 虽然 BIP09/34 在设计时仅应用于软分叉（soft-fork），容易证明这一方案也同样可以用于表达用户对硬分叉方案选择（投票）的状况。

[10] 如果存在硬分叉产生的两条链，那么没有实现手段仅从一条链的块头部（block header）数据确定此链属于哪一个分叉。因此一个 SPV 实现可以被另一个分叉的数据所欺骗。

部署也带来了可观的工作量；

这些问题显著地阻碍了比特币社区执行硬分叉的尝试，导致社区难以就一些关键的实现参数（例如区块大小）做出调整。对于价值-债务网络这样期望表达更为复杂的经济体系的系统而言，这一点是相当致命的。因此，ValueCyber 系统认为有必要将协议共识（至少是其中的一部分）显式化出来，从而可以减少执行改进特别是硬分叉形式的改进所需的工作，并为协议共识的实现（包括软分叉和硬分叉）提供一个统一的模式，从而允许系统对所表达的经济模型中的各种参数进行更多的尝试。

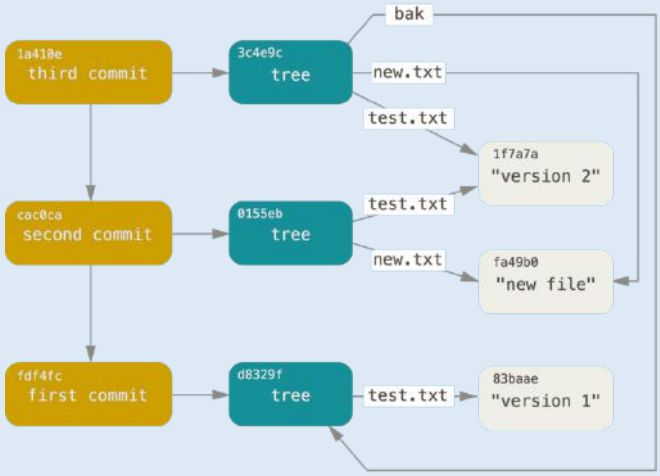
在实现上，价值-债务网络将其所包含的众多参数从实现中显式地抽取出来作为独立的配置模块，因此系统中存在三个关键共识：

- 实现和协议共识，即网络内节点使用的基础协议和相应实现一致；
- 配置共识，对实现中被规定为参数的部分，网络内节点达成一致；
- 历史共识，即节点对当前区块链记录的历史内容一致；

价值-债务网络采用和历史共识一样的方式来处理配置共识的演进。即将其以区块链的形式进行记录并实现分布式存储。节点的实现读取配置模块的所有历史版本，其中每个版本都指定配置其在历史共识中的应用范围（即区块链的高度范围），因此节点可以使用对应的配置模块版本去验证链上的每个区块。

- **是的，就是 Git！**

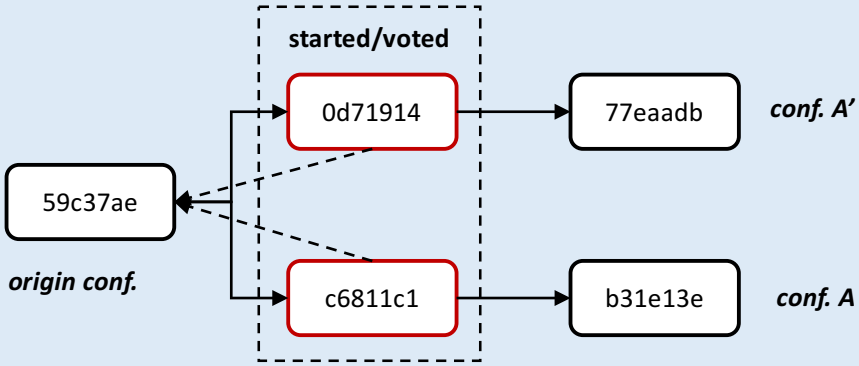
配置系统所使用的“类似区块链形式“的分布式存储方案就是著名的 Git。这个由 Linux 之父所设计的分布式版本管理系统实际上具备区块链所描述的”账本“或“区块”的所有特征[11]。在 Git 中，一个 commit 对象如下图所示[12]，指向一系列特定的文件或索引，以及其过去的历史。任何 commit（包括其历史）都是不可更改的（和区块链一样基于 SHA 哈希算法的碰撞强度）。



Git 的储存仓库可以简单地在任何节点之间同步，从而构成和区块链节点一样的分布式存储体系。虽然 Git 并不是为了数字货币而设计的，不具备足够有效的事务处理性能，然而对配置模块而言这是一个几近完美的方案。

- **配置共识的更改（分叉）**

价值-债务网络节点通常使用下图的流程实现一个新的配置共识：



上图显示了从一个配置共识（origin configuration）出发，全网决议

[11] *Is a Git Repository a Blockchain?* https://medium.com/@shemnon/is-a-git-repository-a-blockchain-35cb1cd2c491

[12] 图片来自于 https://git-scm.com/book/en/v2/Git-Internals-Git-Objects

更改到两个不同的配置 A 或 A‘之一的流程。目标配置（A 或 A’）和初始配置之间使用一个中间状态配置（图中红框的配置）连结。中间配置中指定共识成立的条件，最终配置的 ID 和共识起始时间等信息。节点可以自行选择一个通往最终目标的中间配置，或停留在原始配置。使用中间配置的节点将自动检查区块链的投票结果，决定是否迁移到最终配置或回退到原始配置。软分叉或硬分叉均可使用上述流程，区别仅是硬分叉的中间配置并不要求节点实际更改参数，而仅是确定了迁移到最终配置的时间和条件。

3.3.2 多种事务类型

ValueCyber 的价值-债务网络以比特币为蓝本，但引入新的事务形式以满足更复杂的事务系统的需要。新的事务形式仍然保持比特币事务中基于 UTXO 的 Txin/Txout 结构（对于部分事务，Txout 可以被省略），以及用于构成事务的 script 脚本；同时所有新事务形式也都强制应用比特币中新引入的“隔离见证”机制。

和当前常见的区块链方案不同，ValueCyber 主体的价值-债务网络中仅定义了三种表达的内容，即价值、信用和债务；相对地，价值-债务网络包含了一个功能丰富得多的事务系统。ValueCyber 将资产的描述和定义的灵活性留给具体的生产协作共同体，而致力于设计和实现一个可以容纳更多价值流通模式的区块链系统。

ValueCyber 设计了新的分层事务机制和“只读”引用机制，在 UTXO 框架下部分实现了一个支持键-值存储模式的区块链账本。在 ValueCyber 的价值-债务网络中，多种不同的事务被组织在不同的层次，较低层次的事务对较高层次的事务输出的引用是只读的（亦即允许多次的引用），反之（较高或者相同层次中的引用）则遵循 UTXO 的原则（被引用的输出不能再次引用）。价值-债务网络的层次组织反映了系统内在的运行逻辑。当前价值-债务网络中包含如下从高到低

的层次：

3.3.2.1 管理事务层

价值-债务网络中最高的层次，因此任何低层事务对其中事务的引用均是只读的。这允许管理事务层中的信息以常见的键-值记录形式为其它事务提供服务。管理事务层的事务定义了价值-债务网络中的核心信息，例如准入系统的基础自治群公钥。

价值-债务网络通过在创世块中为准入系统基础自治群的账户（公钥）分配信用单位实现准入系统的初始化。由于最高层次中的信用单位可以任意被引用到较低的层，价值-债务网络中实际包含了一个由基础自治群账户管理的无穷大信用单位源，从而推动系统中的债务相关事务执行。而这些作为源泉的信用单位可以在管理事务层中通过事务转移到其它账户，其效果表现为对准入系统基础自治群中账户的更新。

在管理事务层中定义的原始信用通常包含一组额度不等的输出（例如使用 16 个输出分别表示 2^n（$n : 0 - 15$）个信用单位，从而允许组合出任意的信用额度值。每个输出的管理应当根据其额度大小设置相应的安全性。例如大额的输出通常应当归属于一个多重签名，因此大额的信用分配将由准入系统中的多个成员共同许可的情况下执行。

我们为管理事务层设计了一种名为记录事务的事务形式，在一个 script 运行时环境中提供对任意键-值数据的记录能力。一个记录事务必须指定一个表名，一个键名和一个值；在事务执行时，这些数据都应当首先压入 script 处理器的栈中，换言之，记录事务的有效部分是如下的一段 script：

<table name><key><value>

这段 script 被嵌入 Txin 的 script 当中，并允许通过 script 执行器进行事务合法化的验证。为了提交一个记录事务，用户应当首先提交一个 Txout 包含如下 script 的事务 P：

<3><OP_NHASH256><*hash of record script*><OP_EQUAL>{script of P2PKH}

（系统使用比特币 script 中的保留操作字定义了新的操作 OP_NHASH256，此操作符实际是 script 中 OP_CAT（已经被禁用）和 OP_HASH256 操作符的组合。）之后用户可以通过引用 P，在引用的事务见证中提交记录事务的有效部分。客户端程序可以通过识别上述特定的格式从而解析出对应的记录内容。Txout 部分中的 P2PKH 或其它类似的密钥验证部分限制了每个记录的修改权限。

3.3.2.2 债务表达层

此层用于显式地表达债务和“锁定”的价值(现金)。在 ValueCyber 的设计中，在这一层里的现金 Txout 不应直接进入二级市场进行流通，而只用于执行特定的用途：销毁债务或作为参与 POS 共识过程的凭据。

在正常情况下，在此层中被锁定的价值进入流通过程的唯一手段是通过销毁债务，从而在流通层（见下一节）置换出相应的价值并进入二级市场。但是价值-债务网络本身并不限制价值在债务表达层内部执行常规的交易事务。因此理论上也可能出现一个针对债务表达层的价值的二级市场。然而，所有在场外交易这一层中存在的价值的用户都必须清楚地理解自己这么做的目的，并在进行交易时收到足够的提示和警告。我们也在检讨对直接交易加以限制的可行性。

债务表达层是 ValueCyber 的独创的部分。ValueCyber 通过这一层中记录的价值取代了当前一般加密货币中的决定化币量供应模型（例如比特币通过挖矿逐渐增加系统的币量到一个固定数值），并允许其中锁定的价值通过非决定性的方式逐渐释放到流通层面；而这一释放过程是和系统实际需要的流通币量相关的。另一方面，这一层也为用户（价值-债务网络中的价值拥有者）提供了获利的可能性（通过参与 POS 共识过程取得挖矿收益），从而在系统流动性供过于求的时候对流动性起回收作用。我们将在后文“经济表达”的章节中详细阐述了相关内容。最后，这一层的存在也使系统处理债务事务的实现变得更为简洁。

3.3.2.3 流通事务层

此层是系统中最低的层次，用于表达价值-债务网络中所有要素（价值，债务和信用）的流通。其中的要素（主要是价值和债务）也可以被引用到更高的层次当中。系统在此层中的债务表达过程将在下一节详细阐述。

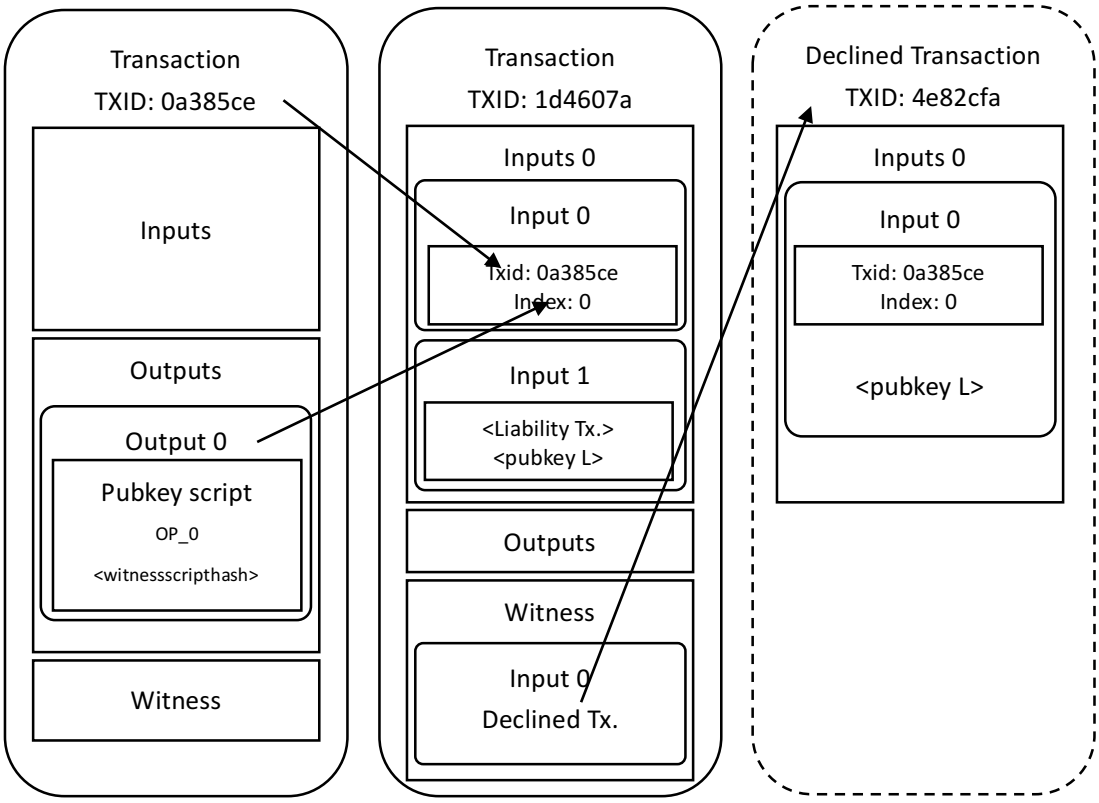
仅从实现上来说，以比特币的事务为原型，流通事务层中所有要素的交换都可以基于单一的规则被统一到同一个事务形式当中（参考后文“一般流通事务“一节）。但是，我们将引用管理事务层的信用输出的事务独立出来，便于矿工亦即价值-债务网络协作共同体执行事务过滤和监管。这一事务被称为信用授权事务。

系统在此层定义一种特殊的“惩罚事务“用于实际上冻结负有过期债务的账户当前所拥有的任何价值（现金）。如前所述，ValueCyber

的实现基于比特币的 UTXO 模型，正常情况下，一个事务中引用另一个事务的输出要求基于事务输出的 script 中指定的公钥信息进行签名。因此事务输出不可能被一个不持有对应公钥的私钥的用户所引用。然而，惩罚事务允许在不使用签名的情况下执行一个引用，只要提供如下证明：

1. 一笔已经被记录在链上的过期债务，其中显式地包含了负债者的公钥 P；

2. 一个**未被记录到链上**的**合法**事务，其中引用了某个链上事务的输出，并且为此引用使用了公钥 P 进行签名



惩罚事务的例子如上图所示，在事务验证时，惩罚事务（0x1d4607a）对所引用输出的合法性验证过程被递归地转移到见证部分中包含的未上链事务（0x4e82fa）的验证。从上述验证逻辑不难

看出这是一个由接收事务的矿工发起的事务。这一事务通过充分的利益激励保证了对债务账户实施有效的惩罚：债务人在负有债务的情况下尝试向区块链发起任何流通事务不仅不会被矿工接受，还会遭受损失事务所动用的资金的风险。惩罚事务在实际的运行中应当是高度罕见的。

在 ValueCyber 的实现中，惩罚事务是一个极为强力的事务，除了可以绕过正常的验证机制引用一个事务输出之外，还会将用于证明 2 中的未被记录的事务永久地标记为一个非法事务，并拒绝任何包含此事务的区块。

这一机制保证了负债者无法通过某种手段控制特定的矿工，在其生成的区块中偷偷包含动用自己账户下资金的事务。因为一旦出现这样的区块，其它矿工可以通过生成惩罚事务将此区块否定，从而撤销作恶矿工所产生的历史。

3.3.3 债务表达

在准入系统一节中已经指出，价值-债务网络区别于单纯的数字货币的关键点在于“债务”的表达。在 ValueCyber 的设计中，我们通过信用概念的实现，进一步引出债务的概念。

如前所述，信用代表了“未来的货币“，即同时对应于其等值的现金和债务；价值-债务网络中信用的源头是在管理事务层中定义的，由准入系统的基础自治群所管理的事务输出。基础自治群在流通事务层中通过信用授权事务将一定的信用额度转移到任意账户（ValueCyber 内部并不区分匿名和实名账户）。这些被转移的信用可以在流通事务层中被进一步转换到现金和债务。实现的流程包括：

- 一个流通事务可以将信用转换成等值的现金和债务，并指定为债务负责的账户；

- 无论在任何一层，将等量的价值单位和债务单位放置到合法的事务中都将冲销此债务；同时使系统中减少相应的现金，这一过程通常是将流通事务层中的债务和价值引用到债务管理层之后执行的；
- 在执行债务转移时，事务总是要求提供等量的信用进行担保，因此债务的转移过程同样处于准入系统的管理之下；
- 在存在到期债务的情况下，为此负责的账户由于债务惩罚事务的存在而实际被冻结；

债务的产生速度取决于信用的发放。后者直接接受价值-债务网络的参与者（即 ValueCyber 的矿工）的约束，因此同样会出现现实中由于系统整体信用额度不足而无法申请债务的情况。虽然这在正常运行的系统中可能是罕见的。

3.3.4 共识机制

价值-债务网络被设计为基于 PoS 机制实现共识的区块链。其中，权益证明（Stake）来自于债务管理层的价值单位。ValueCyber 价值-债务网络的共识方案是一个基于链上数据（chain-base）的方案，即由单个记账者负责生成特定高度的区块。系统实现很大程度上参考了 Blackcoin[13]（这也是国内流行的各类货币常用的一种 PoS 实现方案）。由于当前 PoS 机制部分仍然在开发中，我们再次总结其主要实现要点如下，最终实现方案以系统发布时为准：

- 向比特币区块链聚合共识：按一定的间隔（99 个区块）插入

[13] Blackcoin 的作者将其 PoS 实现升级至 3.0，但是并未给出相应的白皮书。ValueCyber 团队研究了相关代码，此处给出作者的 PoS 2.0 版本实现白皮书供参考 https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

一个基于 PoB（Proof of Burning）共识的区块，以一个比特币区块链上事务的存在性证明获取此块的打包资格，这个独立于 PoS 机制之外特殊的区块可以用于中和链上的事务审查等行为。

- 在确定特定区块的记账者的权限时，随机性来自于比特币区块链当前的状态。

我们采用 Blackcoin 的"Stake modifier"概念计算一个存根（stake）在下一区块中的目标值（target），但是 modifier 所使用的变量来自于比特币当前区块头的哈希值；计算结果值乘以凭据本身的价值单位（coin）来决定是否满足入选条件（Proofhash），从而得到和 Blackcoin 类似的设计：

*Proofhash < coins * target*

对一个特定高度下区块的多个版本，网络将接受引用存根中包含最多价值单位的一个。

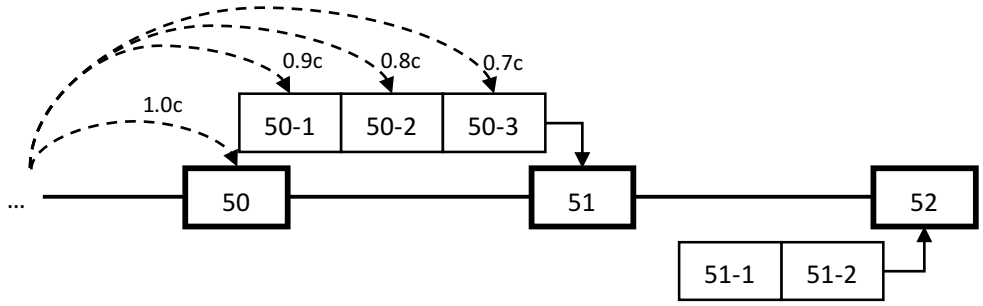
由于 ValueCyber 的实现是基于比特币节点（btcd）进行开发的，我们在实现中保留了和比特币网络通讯和同步比特币区块头的能力，从而可以借助当前全球最强的算力机器来保证 ValueCyberPoS 机制的随机性。

- 债务管理层的价值单位通过特定事务注册为用于生成区块的存根（Stake），并在经历足够长的时间（币龄）后成为候选存根。同时，一个区块中包含的 Stake 量决定了它能产生的信用的最大值。
- 生成区块的奖励是区块内包含的事务手续费（没有额外的奖励）。对一个被网络接受的区块，其生成者获得奖励的 50%，剩余的奖励由下一个生成的区块（引用此区块）获取并进行分配。获得的奖励币值将放置在债务表达层14。
- 我们参考 Sompolinsky 和 Zohar 的方案15，允许多个用户同时提供多个版本的区块。每引用一个前一区块的版本可以获得区块 n（已被接受的版本）所包含价值单位的 2%，上限为 20%，亦即最多被鼓励引用 9 个额外的区块版本。区块 n 中剩余的价值（减去已分配的 50%和区块 n+1 生产者获得的部

[14] 因此系统中假如不存在任何债务，其流动性将是持续收缩的（参考《经济表达示例》一章）。

[15] *Accelerating Bitcoin's Transaction Processing, Fast Money Grows on Trees, Not Chains* https://eprint.iacr.org/2013/881.pdf

分）将被所有引用版本（包括已经被网络接受的区块）的产生者所平分。Sompolinsky 和 Zohar 方案中的 GHOST 算法同样被用于确定主链。一个实现例子如下：



在上图中，不同的用户生成多个版本的链高度为 50 的区块，其中包含最高存根额度（1.0 coin）的版本被接受到主链，对应的用户获得此区块价值的 50%；其它的版本（50-1，50-2，50-3）由高度为 51 的区块的生成者引用，50 号区块价值的另外 50%由接收到主链的 51 号区块生成者和区块所引用的版本的生成者（区块 51，50，50-1，50-2，50-3 对应的用户）平分。同时，51 号区块未被接受到主链的其它版本（51-1，51-2）将被 52 号区块所引用。

- *价值-债务网络是开放的公众链*

  从 ValueCyber 的经济模型出发，ValueCyber 希望所有用户（价值持有者）都参与 PoS 共识过程；因此，我们设计了一个方案允许债务管理层中持有“锁定”价值的用户通过一个智能合约将其价值托管给矿工并分享挖矿所得的收益。借助系统对集体共识事务的支持能力，方案将支持任意数量用户到单个存根的托管和收益分享

3.3.5 一般流通事务

如前所述，ValueCyber 的价值-债务网络采取各种努力以保持共识的效率，以最大程度地扩展共识实现的范围，从而构建一个具备最

广泛参与者的协作系统。因此价值-债务网络将其功能聚焦于系统中的要素（价值，债务和信用）的交易过程，所有流通相关的事务都使用基于比特币交易的形式，并使用下述的原则进行验证：

- 一个事务中每个输出（Txout）包含且仅包含系统三要素即价值，债务或信用的其中之一；
- 一个事务输出的总价值是每个包含价值的输出的总和 - 每个包含债务的输出的总和；
- 一个事务净债务是其每个包含债务的输出的总和；
- 一个事务输入（Txin）的总价值是其引用每个相对本事务在较低层次或同层的事务的价值的输出总和 - 每个较低层或同层事务的债务输出总和；换言之，引用更高层次的事务中包含价值或债务的输出并不影响此事务本身的价值计算，因此除非事务本身有特殊要求，引用更高层次的事务中的价值或债务是无效的；
- 相反，一个事务输出或输入的总信用是其所有包含信用的输出/输入的总和，包括对更高层次的信用的引用；一个事务中包含的净信用是其输入的总信用 - 输出的总信用
- 价值原则：一个合法事务输出的总价值必须不大于事务输入的总价值，减少的部分作为事务的手续费归属于所在区块的矿工
- 信用原则：一个合法事务如果输出净债务，债务的绝对值必须不大于事务的总信用

通过上述规则，价值-债务网络保证了系统中任何债务均存在足额的信用担保；同时，系统的“净价值”（价值-债务）总是保持恒定。例如，系统中一个常见的事务形式是由准入系统提供信用并批准一定量的债务，此事务包含的输入和输出如下表：

输入	输出	总计
信用 P	价值 P - ε 债务 P	总价值（手续费） ε 净债务 P 净信用 P

而一个偿还债务的事务包含的输入和输出入下表：

输入	输出	总计
价值 P + ε **债务 P**	<空>	总价值（手续费） ε 净债务 0 净信用 0

可见，要得到债务 P 和对应的价值，用户必须设法获得相应的信用 P 进行担保，这通常是由用户和准入系统在链外进行协商而进行的：通常地，用户向准入系统中的某个授权代理人提交一个未签名的事务，其中引用授权代理人拥有的某个信用输出，授权代理人签名此事务并提交到区块链上，完成债务的分配。

价值-债务网络在事务合法性验证时同等地对待任何 Txout 中包含的 script，无论此输出是价值，债务或信用。这允许我们在系统内自由地应用任何基于 script 实现的智能合约，从而实现各种链外交易（例如”闪电网络”交易）和跨链交易。确认一个债务输出是可解决的（至少能被一个偿还债务的事务所引用）是提供信用担保的成员的责任。由于债务输出总是对应相应的信用，系统中的债务责任可以简便地进行追溯；坏账也总是能被方便地检测（低于特定区块高度的链上包含的任何债务的 UTXO）。

一个债务输出的 TxOut 通常不会被随意引用（引用此输出不存在利益），因此其 script 部分可以是一个空合约。但是为了能有效地解决一个债务输出，必须保证它可以最终被引用到一个合法的债务惩罚事务，在其中，债务事务可以和一个特定的账户（公钥）关联。我们可以定义下面的 script 为一个标准化的债务格式：

<OP_DUP><OP_HASH160><hash><OP_EQUAL><OP_IF><OP_CHECKSIG><OP_ELSE><EXP_TIME><OP_CSV>

上述 script 是一个 P2PKH 的变体，其中关联了公钥 k。在用户持有对应的私钥并提供签名的情况下，此输出可以在任何时刻被引用。否则，else 之后的 OP_CSV 部分使输出可以在特定时刻之后被任意引用（因此可以被引用到债务惩罚事务）。

很显然，要求每个债务事务都使用上述标准格式和我们期望的智能合约弹性是相互矛盾的，我们设计了名为债务重整化的链外方案来解决上述矛盾。基于重整化方案，在基于上文的事务格式申请一笔债务时，信用授权者并不直接检验此事务（后面称为 T）输出中债务部分的 script，而是要求另外一个位于债务管理层的事务 R，其中合法地引用了 T 中的债务输出部分，并在其输出中将其转换为上述的标准化债务格式。

在事务 T 被批准并上链后，信用授权者保存事务 R，在恰当的时候通过提供另一份信用 P 使 R 合法化并上链，此时流通层中 T 的债务输出被转移到债务管理层 R，并可能被（流通层中的）惩罚事务多次引用。

3.3.6 集体共识

集体共识是价值-债务网络为其上运行的协作共同体提供支持的关键实现。在 ValueCyber 系统中，我们允许任意协作共同体的意志直接实现价值-债务网络上的事务：通过一个应用离散对数密码方案的集体账号，价值-债务网络中的要素可以被归属于协作共同体的整体。一个和此集体账号相关联的特殊见证事务需要共同体内多数成员表决才能被价值-债务网络所认可。

当前我们考虑在价值-债务网络中引入基于离散对数（Discrete logarithm）而不是椭圆曲线数字签名算法（ECDSA）的密码方案。这一密码方案在零币（Zerocoin）[16]中已经被应用过。这一方案可以兼容于扩展的 script 解析器，并应用到系统中任何形式的事务中。

*在离散对数密码方案中，用户选择大质数 q，选择 q 阶（质数阶）模数乘法群 G=$(Z_p)^*$的两个生成元 g，h；并选择选择任意整数 r 作为密钥，生成凭据 c = ⟨tr⟩ * g ^ r mod q。其中 tr 是一个特定的单向函数（trapdoor）tr = h^(e^s + pad) mod p。p, g, h, c 和 e 共同构成了算法的公开部分，并可用其哈希值生成账户地址。在引用输入到此账户地址的 Txout 项时，用户需要在见证部分证明其拥有密钥 r，这通常可以通过一个基于签名的知识证明（signature base knowledge proof）来实现。（如果凭据中使用了额外的单项函数项，必须同时提供 s）*

ValueCyber 在存根中应用离散对数密码的主要原因是保留未来的可能性。基于这一密码方案我们将来可以方便地引入和零币相同的匿名存根方案，以及类似于彩票彩池的混合-再分配方案等。这些实现的计划我们正在检讨中。

*在 ValueCyber 的集体共识实现中，个人凭据部分对应于零币中一个”coin“的表达 c = g^S * h ^ r；集体凭据则是零币中的累加器（accumulator）A = u ^ ($c_1c_2\cdots c_i$) |mod N。由于集体表决中不需要匿名性，其对应于生成一个较为简单的签名知识证明：*

$$\pi = \mathrm{SPK}[R]\left\{(\Sigma r): AccVerify\left((N,u),A,\prod c,w\right) = 1 \wedge \prod c = g^{\Sigma s}h^{\Sigma r}\right\}$$

此知识证明是一个较弱的零知识证明（honest-verifier ZKP），证明同时包含暗门参数S。利用每个账户的暗门参数 S 的特殊形式(S = e^s + 1)，可以得到S mod e = k，k 即参与表决的账户数量。关于此实现更详细的数学内容可参考附录 A。

协作共同体中每个成员通过一个离散对数密码方案生成其个人的一个凭据，一个集体账号则包括此凭据所使用的公共参数，集体成

[16] *Zerocoin: Anonymous Distributed E-Cash from Bitcoin* https://isi.jhu.edu/~mgreen/ZerocoinOakland.pdf

员的数量 n 以及由所有成员个人的凭据构成的集体凭据。在进行集体表决时，共同体内每个成员首先基于个人私钥产生表决内容的见证；表决成员的见证可以共同构成一个单一的集体见证。价值-债务网络将验证此集体见证中包含的成员数量是之前公布的集体凭据中的多数，在验证通过的情况下接受此事务。

比特币本身提供了多方共同认证事务的方法，即 n-m 签名。但是这一方法仅能应用于数量有限的团体（比特币限制最多 22 个签名）。对于成员达到上百乃至近千的集体，即使能通过其它方式拆分并应用 n-m 签名，也是非常复杂且不可靠的过程。同时，逐个验证每个成员的签名将导致系统开销和集体成员数量成正比，因此并不是一个实用的方法。

ValueCyber 创造性地运用密码学方案实现集体共识，这一实现允许节点通过集体提供的单一验证来决定表决是否成功，且其开销是一个常量而和集体成员数量无关，从而将任意成员数量的集体表决事务能力真正地实用化。

3.3.7 基于价值-债务网络的经济表达示例

通过引入债务概念，ValueCyber 的主体网络具备比传统加密货币更强的表达能力，从而可以在数字世界中为现实的经济活动提供除了现金交易以外更多形态的映射。本节从价值-债务网络整体、联合体以及技术创新等不同方面举例阐述 ValueCyber 主体网络的能力。

3.3.8 流动性的解决

和一般的加密数字货币系统相比，价值-债务网络具备三个方式实现价值流通：

- 直接价值交换：即比特币等系统中的流通方式，通过账户持有的价值（币）实现流通；
- 债务-价值交换：账户通过建立债务，生成对应的额外价值

进行流通；

- 直接债务交换：基于债务事务实现债务的流动，即反向的价值流通；

债务-价值交换是 ValueCyber 系统在价值流通中最为重要的创新。一个货币系统如果应用于资源和价值流通，那么其价值总量将对应于一个固定的流通规模，即：

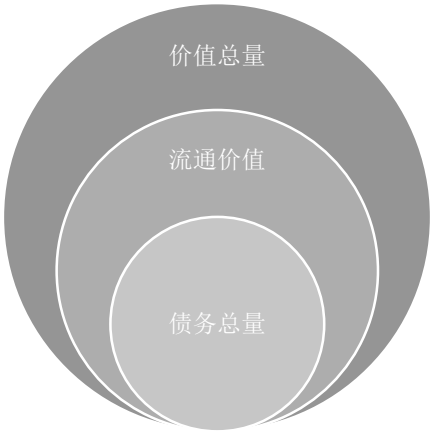
流通规模 ≦ 价值总量

流通规模的改变将引起价值总量的变化，如果系统中当前货币总量不发生变化，则将导致货币的单位价值改变，表观上即由于供求关系改变造成的货币币值波动，而这对货币作为流通符号的功能是不利的。

因此，为了适应流通规模的快速变化，一个货币系统必须相应地改变其投入流通的货币总量，才能有效地保持单位货币的价格。当前的常见的加密数字货币系统并未实现这样的机制，它们通常使用一个短期内相对稳定，长期则以固定的方式增长的总量，这导致其在长短期内都不具备有效地调节总供应量的能力，因此通常会有一个随供求关系而显著变动的价格。

ValueCyber 系统的价值-债务网络通过债务管理层和债务-价值交换为基础实现了币供应量的调节。这是因为债务管理层中的价值无法直接和外部交换，因此系统当前可流通的价值总量需要扣除在债务管理层中的价值。同时，系统可以通过债务-价值交换向系统中注入临时的流通价值。因此系统中实际参与流通的价值由三部分组成，如

下图所示：



流通价值总量 = 价值总量 - 债务管理层价值总量 + 债务总量

价值-债务网络中主要通过扩大或缩小的债务总量来调控流通价值总量，而在债务不起作用时，仍然可以通过将流通价值吸收进债务管理层或从后者释放出来以保持调控：当外部对流通结算的需求增长时，债务-价值交换活动将随之而活跃（债务生成速度增加），从而向系统注入更多的流动性。而当流通结算需求降低时，债务-价值交换活动减少，相应地债务减少，导致一般流动性迅速减少，同时，持有多余价值的用户将更倾向于将价值转移到债务表达层以便以获取稳定的收益，两个因素的共同作用可以迅速减少流动性。通过这一可调节的流通价值总量，价值-债务网络实现其和流通规模的有效匹配：

流通规模 ≦ 流通价值总量

因此，将价值-债务网络用于支撑生产和流通过程，其结算单位的价格稳定性和其它加密货币相比具有显著的优势。基于ValueCyber的流通系统将具有更大的弹性来支撑急剧变化的生产和市场，同时也更接近于现代经济体系的运行模式。

处于债务表达层的价值单位由于可以作为参与 PoS 共识机制的凭据通常称为“挖矿券”。这部分价值通过债务偿还方式进入一般流动性是价值-债务网络中特有的设计。在对价值需求增加（币价上涨）时，挖矿券相对往往具有更低的实际购买价格，导致这部分价值的持有者倾向于和债务人执行下面的协议：

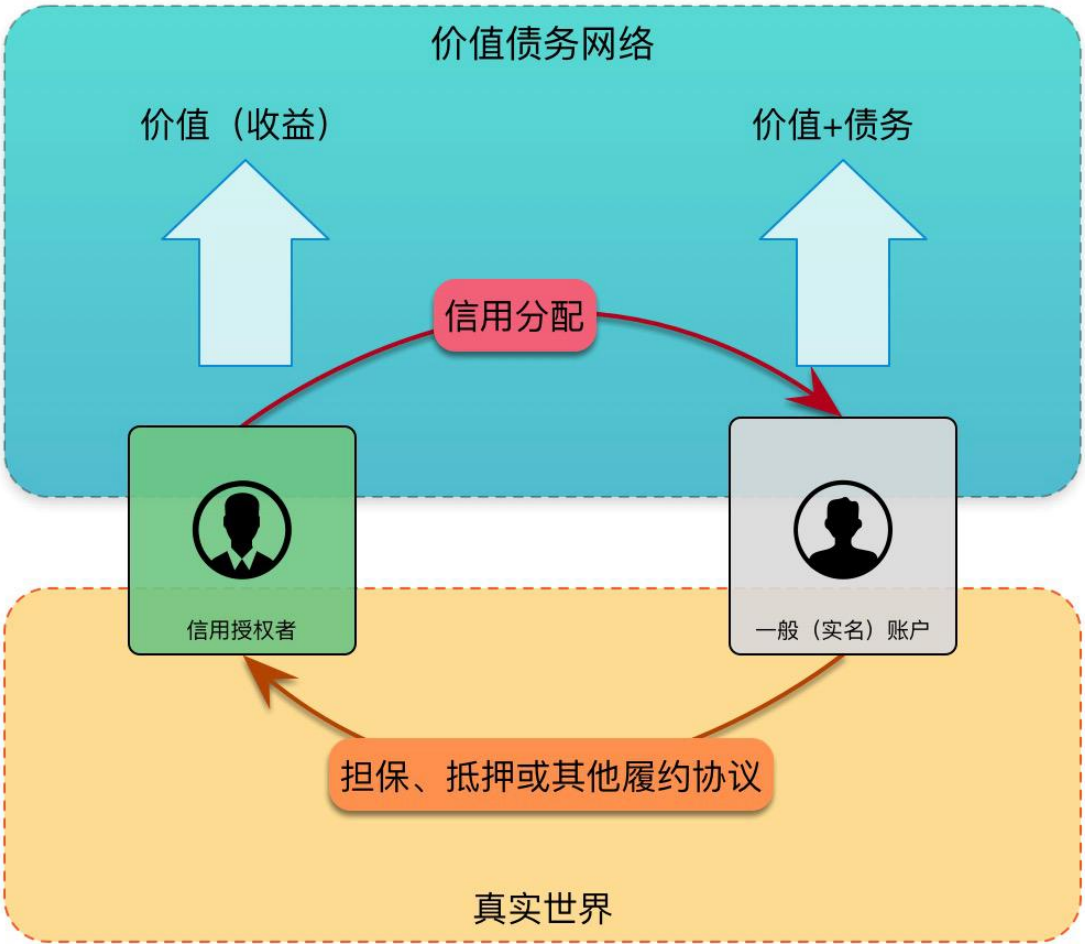
- *债务人向挖矿券持有者转移 a*L 单位在流通事务层的价值，换取挖矿券持有者为债务人在债务管理层清偿 L 单位的债务，其中 $a < 1$*

上述协议是挖矿券恢复系统内流动性的唯一途径，这构成了共识机制的参与者批准债务而不是囤币待涨的原动力。

3.3.9 债务管理

价值-债务网络中债务总量的确定、分配（限额）以及保证债务被履行可能是实现 ValueCyber 全功能运作最为困难的一环。正如我们之前论述的一样，这些工作在 ValueCyber 中被移动到价值-债务网络外部，由准入系统负责实现相应风控系统、担保系统以及债务义务在系统外的追溯能力。而系统内部仅需将未能履行债务义务的账户将被清除出价值-债务网络，并由准入系统将其债务最终消除（销坏账）。

一个最基本的准入系统实现模型可能是基于外部价值的全额担保的系统，如下图所示。信用授权者的利益在于为用户生成债务时的服务费用；对未在系统内履约的债务，信用授权者可以通过从系统外部输入价值（例如从二级市场购入）来进行抵消。



价值-债务网络中并不存在一个“定向”于特定账户的债务概念（亦即，所有债务的债权都属于价值-债务网络全体）。这基于一个明显的推论，即一个账户在系统内除了系统本身，不存在其它使债务持有人履约的强制力。因此，如果考虑通过系统的强制力实现债务人的向特定账户履约，实质上等同于债务人直接向系统本身履约。再进一步说，特定于一个账户的债务协议实际上只存在于系统之外：在系统之内则表达为两个账户之间的价值转移，正如上图所示。在整体上，这对应于一个价值和现实世界中债务的交易过程。（假如交易在系统外的部分不是现实世界而是另一个区块链系统，那么这就是一个跨链交易。）

即使是上述的简单全额担保系统在现实中也有其应用意义。例如当担保物为某种法定货币时，相当于授权者实现了相应货币的在价值-债务网络中的数字化，或建立一个两者的二级市场。这个过程只需要得到更高阶的管理者（如准入系统的基础自治群）的许可，并为其分配一个不会显著影响价值-债务网络总量的信用额度，而不需要信

用授权者预先储备价值-债务网络中的价值单位。

3.3.10 信用控制和非确定性共识

如前所述，价值-债务网络由准入系统决定网络中的债务总量和对应的流动性价值总量。对准入系统行为合理性的审查则由基于价值-债务网络的协作共同体亦即矿工共同进行。在具体实施中，矿工仅需要控制网络中信用的发放速度，亦即信用授权事务在单位时间内进入价值-债务网络的总量。ValueCyber 将这一控制权放置到系统的共识机制外部，通过协作共同体成员分别执行的非确定性机制，实现弹性的共识。

价值-债务网络共识机制中仅对信用授权事务实现一个基础的限制，即区块中包含的信用输出总量不可超过生成此区块的 Stake。而系统实际的信用和债务增长量均由非确定共识实现。这些策略可以在系统之外持续改进和演化，当前 ValueCyber 提供给协作共同体（矿工）的非确定性共识策略包括：

- 基于流动价值总量的信用发放速度控制：策略将是基于上述变量的函数。而在上述变量达到特定上限时，禁止任何新信用发放事务；
- 信用储备量控制：准入系统通常会储备一定的信用值以应对突然的需求峰值，但这一数量应当在一个合理的范围之内，例如当前流动价值总量的 10%；
- 基于未偿付的债务寿命的平均值的控制：通常应当和 PoS 机

制中 Stake 恢复有效的周期相等17；

- 紧急开关：由用户直接发送指令立刻禁止信用发放事务；

在区块链系统中，非确定共识即由每个记账者对其负责打包的区块内事物独立进行选择得到的结果；共识的整体效果取决于所有记账者策略的总合。比特币的事务手续费比率即是一种典型的非确定共识。ValueCyber 将此实现扩展到价值-债务网络的核心部分，即对信用发放速度的控制，通过协作和市场来获得系统整体的最优策略。

价值-债务网络通过下列要素使矿工有动力去应用一个合理的策略来执行对信用的审查：

1. 矿工需要债务偿付机制来使其在债务表达层的价值（挖矿券）恢复流动性，这使其不会完全拒绝任何信用的产生和债务的发放；

2. 偿付机制要求“好“的债务（能被清偿的）而非坏账，因此矿工会监督准入系统的债务质量，即使在受到准入系统的贿赂的情况下也不放松对债务质量的要求；进一步而言，矿工实际上将会从信用发放过程中获得好处（见下面的讨论）

3. 由于信用的产生额度和 PoS 共识的投票权成正比，矿工的策略将能有效地控制信用的发放速度和系统的债务增长规模；最严重的攻击方式可能是准入系统将其储备的信用值全部变成坏账，这也意味着准入系统和价值-债务网络合作的彻底决裂；由于信用储备量控制策略的存在，坏账比率不会超过策略规定的流动价值总量比例（如10%）。相对于准入系统的重要性，造成这一损害的程度应当是可以容忍的。

[17] 由于区块内 Stake 的量决定了信用的量，亦即可产生的流通单位的最大值；易推出当一份债务的周期和 Stake 的周期相同时，系统的流通单位总量在长期来看和总币量相同；

我们设想在价值-债务网络正常运行的状态下，矿工将从准入系统中获取利益，作为向其提供信用的代价：准入系统通过债务的利息获取收入，然后将这些资金以可任意使用的形式与授信捆绑到同一个事务中，并由矿工选择并打包进区块。事务中的利益部分由生成此区块的矿工获得。相对于事务手续费的微量收入，这将是用户将资金注入债务表达层并参与挖矿（共识）的主要动力：即一个来自于系统债务利息的稳定收入。

3.3.11 从个人到集体

ValueCyber 的集体共识事务设计允许在更小范围内建立更紧密的生产和经济共同体。这些共同体的数字世界映射（例如一个联盟链）可以在 ValueCyber 中以一个整体形式存在，拥有从属于集体的价值和债务。当前的集体共识事务为共同体贯彻其集体意志提供了最为基础的实现方式即“多数表决”。ValueCyber 团队未来将进行持续的探索和开发，为共同体事务提供更多的实现支撑。

共同体在 ValueCyber 上产生一个或多个集体凭据来管理共同体所拥有的价值（货币）和债务。不过，不同于“基础自治群”的概念，价值-债务网络中的节点并不关心共同体内成员的变化状况。例如，共同体中一部分成员 S 可以拥有一个独立的凭据，此凭据下拥有的价值的管理只需要这个成员的子集 S 的多数决。

一个共同体可以通过其闲置资金的整合和更高整体信用为共同体中的个体提供提供更为强力的支持，这将大大加强小生产者对抗市场风险和意外的能力。

3.3.12 新的数字金融形式

ValueCyber 系统通过实现债务概念允许更多金融形式在价值-债务网络上的数字化实现，其中之一是完全离线的支付方式（类似于传统金融体系中的支票系统），并可以进一步发展出更为简单高效的离

链支付和结算方案。

和比特币的离链（off-chain）支付方案即“闪电网络”（lightning network）类似。一个账户可以将其信用额度分配到有限的结算中心（或者，由结算中心为账户分配信用额度），并只需要在结算中心内部同步其债务状况，结算中心随后可以通过彼此的结算流程定期地更新账户在全网络中的债务状况，从而有效地降低用户的交易信息在全网络中的同步开销。更进一步，基于同态加密（Homomorphic encryption）方案的债务事务表达允许账户的多笔链外交易在结算（上链）时被合并。

四、ValueCyber 迭代计划

ValueCyber 项目的主要实施计划和里程碑如下：

ValueCyber 的未来迭代计划

作为第三代区块链技术，ValueCyber 的未来迭代包含三个部分，一是代码本身的迭代；二是基于价值-债务网络的高灵活性商业应用迭代，三是基于生产网络的高扩展性商业应用迭代。

- ValueCyber 底层架构的迭代

当 ValueCyber 代码本身出现漏洞，通常可以在神谕账户和矿工联合体的共识下进行系统升级，出现的漏洞需要经过代码委员会进行分析、测试和审核，提交至决策委员会报备，当出现以下重大漏洞（不限于）将采取系统升级：影响价值-债务网络的重大安全问题；影响生产网络的重大安全问题；可能会导致用户资金丢失的重大安全问题等。

- 第三方运营者的商业迭代

价值-债务网络的应用主要体现 ValueCyber 系统的高灵活性，它需要大量有“自由定义业务”需求的第三方运营者加入，ValueCyber 将选择包含风险评估机构、小额贷金融机构、典当机构在内的各类第三方运营者合作，进行商业应用的迭代，应用由第三方主导，ValueCyber 提供技术支持。

- 第三方开发者的商业迭代

生产网络的应用主要体现 ValueCyber 系统的高扩展性，它需要大量有“自由开发程序”需求的第三方开发者加入，ValueCyber 将选择包含各行业联盟和协会组织、各类企业和个人在内的各类第三方开发者合作，进行商业应用的迭代，应用由第三方主导，ValueCyber 提供技术支持。

五、应用场景

ValueCyber 通过对价值网络中的经济共同体提供流动性赋能，释放了经济共同体中的资产价值，优化了经济共同体之内、经济共同体之间的生产关系，具备广泛、普适的应用服务场景。

5.1 场景一：知识产权 IP

知识产权（IP是intellectual property的缩写），全称为intellectual property right，是一种无形的财产权，也称智力成

果权，它指的是通过智力创造性劳动所获得的成果，并且是由智力劳动者对成果依法享有的专有权利。

随着知识经济的发展，IP已经成为市场竞争力的核心要素。虽然我国对IP的保护极为重视，并且也取得了不错的成绩，但是随着互联网的迅猛发展，信息传播成本几乎为零，创新成果极易被他人“复制”。如果不用严格的IP保护制度进行约束，企业创新投资就很难得到应有的回报，将严重打击企业创新的积极性。各种盗版和无视IP，以及侵蚀原创权益的行为，已经成为IP产业尖锐的痛点。

近年来，IP概念被广泛热炒。《滚蛋吧!肿瘤君》由漫画IP转化而来，《小时代》、《何以笙箫默》由小说IP转化成电影电视剧，《十万个冷笑话》由漫画到动画再到电影，总票房超过了1亿。伴随着IP概念的火爆，各大IP的价格也在水涨船高。但是，对于IP保护方面却存在诸多真空地带和问题，IP所有者的价值也未能得到充分体现。

ValueCyber可以通过区块链技术结合创新的商业模式有效解决这些问题，就是为解决这些商业痛点而设计的，是一个专门为数字IP打造的区块链商业应用平台。平台基于区块链技术构建溯源清晰、产权明确、信息不可能篡改、资产流通自由等特征实现IP资产的价值交换，旨在解决IP资产融资难、商业化难和产业化难等问题。

ValueCyber作为全球数字区块链商业应用的倡导者，以区块链技术构建去中心化的IP发布交易平台，去除中心化商业机构，真正

做到创作者与消费者的直连，实现IP在互联网上的P2P交易。同时，ValueCyber还能实现IP的确权、打赏、交易、众筹、众包等应用。采用消费者分享评价推广模式，让真正的好作品得到最大的认可和回报，让分享者既能消费好的作品，又能在分享评价中得到收益，也许这才是未来公平、公开、公正的IP分享和消费平台。

ValueCyber的定位是为未来商业落地而构架的一个基础公有链，ValueCyber 将重点聚焦在基础区块链及应用开放平台的建设上。ValueCyber 的应用落地领域和场景非常广泛：发明专利应用、商标应用、著作权应用、音乐行业应用、视频行业应用、软件及设计行业应用、传统书画、艺术品等行业应用、公证行业应用、网络写作及自媒体应用、教育培训行业的应用、其它领域。

5.2 场景二：服务农业产业化联合体

农业部、国家发展改革委、财政部、国土资源部、人民银行、税务总局于2017年10月25日印发了《关于促进农业产业化联合体发展的指导意见》。农业产业化联合体是龙头企业、农民合作社和家庭农场等新型农业经营主体以分工协作为前提，以规模经营为依托，以利益联结为纽带的一体化农业经营组织联盟。《意见》中明确要求，农业产业化联合体要“健全资源要素共享机制，推动农业产业化联合体融通发展”（一）要发展土地适度规模经营（二）引导资金有效流动（三）促进科技转化应用（四）加强市场信息互通、（五）推动品牌共创共享。

农业产业化联合体完全可以在ValueCyber中表达：

第一步：农业产业化联合体组织关系数字化映射。农业产业化联合体之内产业链关系，可以在ValueCyber支持下，在数字世界映射成一个联盟区块链，并以一个整体，在ValueCyber中以经济共同体的形式存在。

第二步：农业产业化联合体服务能力建立。农业产业化联合体在ValueCyber中完成资产数字化后，拥有从属于集体的价值和债务，可借助ValueCyber的表达能力，在数字化资产的背书下，在ValueCyber中获得流动性支持，从而完成海量农业固定资产的流动性释放，提高农业产业化联合体的融资效率、降低融资成本。

第三步：应用场景创新，助力实现C2B按需定制生产关系。考虑这个共享农庄的场景：例如，由生产网络服务企业余粮宝在ValueCyber基础上，构建服务农业产业化联合体的农业价值网络，首先在海量城市周边休闲农场、有机认证企业的会员服务中落地农产品众筹及溯源。传统的众筹及溯源模式中，消费端的合约及众筹预订现金流无法在农业产业链中无阻断、原子性的流转，从而无法驱动生产环节的生产投入计划，这就间接加大了各个环节的信任成本、库存成本，并引入了生产过程的开放及不确定问题，由于生产过程开放、不确定，最终产品的食品安全性、质量稳定性、产品标准化等都不确定，解决食品安全的溯源工具就不具备可信的逻辑基础。引入基于ValueCyber的农业价值网络后，用区块链统领产业链，消费者众筹款达到智能合约中约定的触发条件，自动触发产业

链上的既定商业合约交割，从而确保了生产计划和投入品的确定性，产品质量、提高了产业链上资产、资金的周转效率，食品安全等问题也就得到了解决。同时，反映真实产业链运转的信息，都在区块链中记录在案，以溯源信息的形式呈现给消费者。

这个体系建立后，农业产业化联合体内的企业实现了现金流优化，在有订单支撑的情况下，以农业产业化联合体集体信用在ValueCyber上获得流动性支持，交付给客户合格的产品和服务。

5.3 场景三：手游行业

行业格局

手游产业链的三大环节，研发商、发行商和渠道商，这三大环节决定了中国手游市场的格局。研发商是整个游戏产业链的上游环节，对厂商的创意和技术要求极高， 研发商较为分散，规模不一，基于各类平台提供游戏内容，是整个游戏生态的创意和价值源头。 游戏发行商将产品从研发商推向分发渠道，专注于游戏的调优及推广。游戏分发渠道掌握流量入口以及大量玩家数据，拥有较大行业话语权，移动游戏分发渠道大多被互联网巨头垄断，呈现逐渐整合态势。

手游用户具备社群基础

应用商店、微信 QQ 等社交平台、朋友推荐成为用户获取游戏咨询的主要渠道，分别占到 65%、 43.9%和 36.7%。其中微信、 QQ 等社交平台用户基数大并且活跃度高，朋友间相互推荐成功试玩的几率非常大。厂商游戏推广渠道趋于多元化，用户获取游戏资讯变得容易。

手游行业的问题

1.渠道结算问题： 渠道诚信度下降，伤害中小游戏开发商

虽然近几年手游行业迅猛发展，手游付费增长很快，但进入 2016 年以来手游市场的游戏开发商却叫苦连连， 也显现出了手游渠道的诸多负面问题。个别大渠道开始拖欠游戏开发商分成款项，而这种拖欠目前已蔓延到了多个渠道。 拖欠游戏开发商分成款，其根本原因是渠道自身的推广成本越来越高， 利润微薄。

2.获客问题： 渠道用户粘性下降，移动入口多元化。

当下用户获取手游资讯的方式越来越多，除了传统手游渠道，玩家可以通过无数种方式获得自己想玩的游戏。无论是广告、微信公众号、流行 App，还是微博、贴吧、朋友圈分享，都比传统渠道更简明和直接。

价值网络对手游行业的作用

1.游戏开发商可直接触达用户

游戏开发商可以通过价值债务网络的跨行业体系实现游戏的快速分发，获得大量的精准用户。游戏开发商可以通过平台活动奖励提升游戏的参与度和活跃度。

游戏开发商可以在项目早起获得启动资金和分成结算，在项目发起时获得用户的及时反馈。

2.游戏玩家可免费试玩，并参与交易

项目采用特有的授信机制，可实现游戏玩家购买游戏前先授信试玩，玩家满意后才进行下载及付费。

游戏玩家发现好玩游戏后可以分享给好友，好友购买游戏或游戏内充值后推荐者可以获得代币奖励。

游戏玩家可以通过玩游戏和游戏充值获得代币，代币可用于参与平台的发展路径投票、虚拟道具交易及玩家间交易。

3.渠道可以直接建立产业链

项目将为渠道附能，支撑渠道打造一个游戏行业的产业链。在基本功能搭建完毕系统成熟后，项目将会把试玩、分享、激励、结算等功能模块逐步对所有渠道开放，共同建立游戏行业的价值链。

价值网络对手游行业的升级改造

利用基于区块链技术研发的下一代加密数字货币，改变现有的手游产业链的经济循环系统，使开发商、发行商等供应方能相比以往更快速的获得分成结算，使游戏推广、玩家等消费方享受原有收益又能获得项目长期增值收益。

最终以价值-债务网络为基础，打造一个游戏行业的生产网络，在链上打通投资、 研发、发行、 推广、运营等各个环节，连接投资商、研发商、发行商、渠道商、广告商、运营商、支付商、玩家等各类机构和用户，实现游戏分发、试玩、下载、激活、充值、 电竞等各方面服务的生态系统。