DHG：面向全球物联网的下一代区块链应用平台

摘要

DHG(Distributed Hybrid Global)是一个区块链技术综合应用平台，旨在打造下一代区块链物联网系统，中本聪发明了比特币之后，虚拟币、区块链行业获得飞速发展，由最初的对于“币”的探索，转为当前对“链”的探索，下一步，将是朝着“网”的方向发展，DHG 的终极目标就是打造一个区块链网络系统，以作为物联网底层协议。

DHG 是一个分布式数据库系统，数据自动在全球各个节点备份，并借助密码学以及博弈论等，由全球矿工共同维护网络安全，任何个人或者组织都很难篡改系统数据，因此他是一个信用系统。借助侧链，混合挖矿，图灵完备性虚拟机等，用户可在 DHG 上发布智能合约，智能合约一旦发布，将严格按照既定规则运行，因此 DHG 是实现自动化和智能化的基础，同时也是物联网发展基础协议。

DHG 首先是一个数字资产管理系统，任何人可借助 DHG 发布基于区块链的数字资产，数字资产借助 DHG 自由流通于区块链，不受发行方控制。DHG 同时也是 DHG 区块链网络的特定内置代币的简称，总量恒定，是 DHG 网络的价值传输媒介及区块链云计算燃料。

侧链是 DHG 的核心部分，借助双向挂钩及混合挖矿技术，代币可在主链和侧链间以特定形式流转。侧链不仅分担主链的负担，使区块链系统更加灵活轻便，同时也是实现去中心化应用（DAPP）的方式之一。

智能合约是区块链的核心应用，同时也是自动化，智能化基础，考虑到以太坊虚拟机（EVM）发展越来越成熟，DHG 将在恰当时机兼容 EVM。

DHG 顺应区块链发展潮流，在虚拟币和区块链发展基础上，定义并扩展区块链网络协议，打造面向全球物联网的区块链应用平台。

1. 区块链发展

2008 年，由次贷危机引发的金融危机席卷全球，人们再次意识到传统金融系统的不足，并设法对其改进和优化。同年 11 月，一位署名中本聪的密码专家发表了那篇著名的比特币论文，宣告比特币的诞生，当然，后来大家都知道，同时伴随着区块链的诞生。在论文里中本聪只是将比特币定义为去中心化的点对点支付系统，如今区块链的发展早就超出了支付范畴。

第一代：币

比特币是一套分布式自治系统，是应用数学和金融经济学的完美结合，如果你仔细研究这套系统，你会发现，他同时囊括了央行（发行货币），商行（支付）以及作为货币本身的职能。在这套系统里，天才的中本聪采用非对称密码来解决比特币的所有权问题，采用 UTXO 模型定义了一个“币”的概念，并用区块链解决分布式交易验证的问题。工作量证明方式（POW）维护系统的正常稳定以及安全，在博弈论的作用下，所有矿工维护统一的区块链，以最终解决双重支付问题。直到今日，比特币依然是无可动摇的数字货币龙头老大位置。

莱特币对比特币的改进很少，但引发了算法改进热潮，催生了很多数字货币。如果将比特币视为一场社会实验，众多山寨币则是一种比特币实验，莱特币激活隔离验证，再次印证了这一说法。

在众多一代币中，有一个发展分支目前依然换发着蓬勃的生命力，即主打匿名的数字货币，Dash、Zcash 便是其中的代表。

DHG 将吸收多众多虚拟货币先驱的优点，综合应用于共识机制，算法，隐私等。

第二代：链

当人们逐渐缕清比特币和区块链的关系之后，视野顿时一片开拓，发现比特币仅仅是区块链的一个应用，区块链还会有其他应用，由此，整个行业的发展重心由“币”转向“链”。如今很多人都知道，可以将区块链视为一个分布式数据库，该数据库的核心特点是沿时间轴记录数据与合约，并且只能读取和写入，不能修改和删除。

比特股（Bitshares）率先奏响区块链探索的号角，以太坊（Ethereum）则真正让这场革命发生质变。以太坊不但继承比特币的诸多优点，同时引入了很多创新，他是一个智能合约平台，同时也是一个分布式应用底层协议。

以太坊最迷人的地方莫过于其几乎具备“图灵完备性”的虚拟机（EVM），当然，由此也带来了巨大的技术复杂性以及容错成本，以太坊为此还出现过硬分叉。如今社区普遍认为，这套体系还远远不完善，有待优化的地方还有很多，区块链和智能合约的探索之路还很漫长，这也是 DHG 由来和机遇。

下一代：网

在过去 8 年多时间里，数字货币产业已由币发展进入链的时代，那下一步将如何发展呢？

互联网诞生至今不过 30 年，如今已改变了全世界，人们普遍认为，互联网之后，下一个网络是物联网，物联网已被提及多年，更有 IBM 孜孜不倦的在研究，但始终没有获得实质性进展，甚至物联网为何物还不能对其做清晰描述。直到区块链出现之后，局面才被打开。

造成该困境的原因之一是，过往的技术，我们无法实现真正的自动化，而比特币这套已被证明切实可行的分布式自治系统（DAO）正好完美的解决了这个问题。DAO 提供了自动化的基因，从而可作为物联网的根基。

如今物联网和区块链总是被捆绑在一起讨论，展望未来无处不在的物联网，这很令人兴奋。因此我们有理由相信，区块链的下一个进化形式是网络，众多的区块链不会再彼此截然分隔。DHG 就是要打造这么一个区块链网络。

2. DHG 设计理念

区块链技术被认为是互联网发明以来最具颠覆性的技术创新，它依靠密码学和 Hash 函数，博弈论等应用数学基础理论，在无法建立信任关系的互联网上，无需借助任何第三方中心的介入就可以使参与者达成共识，以极低的成本解决了信任与价值的可靠传递难题。

自比特币之后，很多区块链项目如雨后春笋般涌现，其中很多项目都有突破性创新，或者底层协议作创新，或在应用层面做创新，从整个行业来说，这些区块链项目有具备实验性意义。DHG 的设计将综合考虑、整合众多项目的优点，并做一些开拓性探索，引领行业迈向下一代区块链网络。

核心理念

DHG 在设计上将保留比特币所有核心特征，比如 P2P 系统，去中心化，非对称密码保证资产专属所有权，匿名性，无国界、全球化应用等。DHG 保留比特币系统最有价值的部分，秉承作为信任网络的本质，实现低成本价值传输。

为应用而生

区块链发展已经进入应用发展时代，每个人都在试图将自己的从事的工作跟区块链结合起来，充分发挥区块链优势。然后当前区块链项目存在很多瓶颈，比如比特币，容量成了阻碍其发展的核心问题，为了适应大规模应用，DHG 顺应时代发展，服务于应用，将重点在如下几方面做优化。

交易容量

比特币平均每秒 5 笔交易的处理速度已经严重阻碍其发展，目前网络有时拥堵甚至已达 15 万笔，扩容成了当务之急。当前的处理速度俨然不能承载全球化发展以及资产数字化的趋势。为了解决这个问题，DHG 将采用更加合理的数据存储架构，以及交易历史的清理机制。

交易速度

同样，比特币 10 分钟一个确认的设计也让人诟病，DHG 必须要能实现秒级甚至更快的处理速度。这方面，以太坊测试取得了突破性进展。为了解决这个问题，DHG 将在共识机制上做改进。

可行性

DHG 的最终目标是打造下一代区块链网络，主要涉及侧链技术，混合挖矿，SPV 验证方式，以及智能合约等，这些技术都已经被虚拟币社区论证，比如侧链技术，被认为是 2015 年提出的最重要的比特币升级协议之一，已经有包括 Blockstream 在内的众多个人或团队在努力开发中，相信不久就会投入实质性应用，混合挖矿业以是在投入使用的成熟技术，SPV 是中本聪在创世论文中就论证的，而智能合约则可以借用以太坊的虚拟机（EVM）或比特币内置的脚本系统实现，因此这些核心技术具备可行性。

DHG 团队秉承“站在巨人的肩膀之上的”的开发理念，充分吸收其他区块链项目的优点，并结合自己的创新，践行确实可行的方案。

易用性

比特币官方客户端正在变得越来越不好用，因为数据量不断膨胀，个人用户不得不被迫放弃官方客户端，这个从侧面削弱了比特币的安全性，因为用户为了便捷，不得不将币放在交易平台等中心化服务器上。

对于以太坊来说，则更加难用，且不说复杂的智能合约（需要对 EVM 以及 Solidity 等高级语言足够熟悉），即便是简单的交易也需要安装复杂的客户端才能实现。这些难度都无意间推开用户。

DHG 将提供多样客户端，除了 PC 端钱包，还包括 APP，以及网页端等，并可以

处理简单的脑钱包机制以及钱包备份、恢复机制。方便易用是 DHG 的首要设计需求。

兼容性

比特币是目前最成功、最稳定的数字货币系统，其中的很多设计理念都已被证实确实可行，DHG 特别重视与比特币网络的兼容性问题，比如借鉴比特币的 UTXO 模型，以及地址构造流程，中本聪脚本（Script）系统等。

以太坊的虚拟机 EVM 正在变得越来越稳定，以太坊社区开发团队正在变得越来越庞大，DHG 将全面兼容 EVM，能部署在 EVM 上的智能合约，可以不做任何修改就能在 DHG 上运行。

稳步成长

DHG 的发展前景是令人着迷的，但不能一蹴而就，与其一开始提供复杂完整的系统，我们选择稳步前进的开发路线。以太坊硬分叉就是一个借鉴，相对而言，中本聪脚本一开始也提供了很多操作码，也能实现图灵完备，不过开发团队后来慢慢禁掉了很多操作码，只开放一些常用操作码，此举换来了比特币 8 年多的稳定运行。

DHG 采用一步一个脚印的发展策略，总体而言，开发分三步走，首先将运行主链，主链运行充分稳定之后，将开放侧链，最后择机开放智能合约功能。这三步走过之后，DHG 将初具区块链网络雏形，然后进入应用驱动型发展新篇章。

3. DHG 技术概述

比特币，以太坊等都是一个开源项目，其底层协议和技术实现方案都是公开的，因而我们可以吸收他们的优点，结合自己的扩展，开发新的区块链。

共识机制

共识机制是区块链系统的核心，共识机制与系统的安全性，稳定性，以及各种效率息息相关。例如比特币，采用 POW 共识机制，至少有 3 个作用，一是产生新区快，保证系统正常运转，二是维护系统的安全，算力越大，意味着越安全，第三个作用是分发货币。

人们在共识机制上的研究下了很多功夫，各种共识机制相继被提出来，其中较为出名包括 POW，POS，以及 DPOS 等。

POW(Proof of Work)是比特币率先使用的共识算法，核心理念为通过算力来争夺

区块铸造权，其过程很简单，就是让机器不断做 SHA256 运算，以找到符合难度的运行结果，合格区块：

Hash(Block_Header) <= Target

其中 Target 由全网难度决定，对于每个矿工来说是一样的。

后来，有人提出了另一个更为环保的共识机制，且完全依赖系统内部解决，不耗费能源，核心理念为依据余额争夺区块铸造权，其过程为通过消耗币龄以找到符合难度的区块，即通常所说的 POS(Proof of Stake)，合格区块：

ProofHash <= Balance * Age * Target

Balance * Age 即币龄，但是 Age 的引入导致很多用户可以屯币，每过一段时间才开启客户端铸币，持币人获得了收益，但是并没有起到实时维护网络的功能，因此 POS 发展到 3.0 阶段时，去掉了 Age 元素，以激励更多节点实时在线铸币，区块判定条件为：

ProofHash <= Balance * Target

POW 耗费算力，耗费能源，但系统的安全性比较强，POS 不浪费能源，但其安全性能还没得到公认，而且公平性也存在一些争议。不过最近出来的很多新项目都纷纷抛弃了 POW，POS 得到越来越多认可，经过中和考虑，DHG 使用 POS 共识机制，而且是 POS3.0，权重抛弃币龄的概念，只依赖币量。

代币模型

存在两种常用的代币模型，即 UTXO（unspend transaction output）模型和 Account 模型。在比特币社区里，Transaction 被简称为 TX，所以上面这个短语缩写为 UTXO。一般而言，我们最熟悉的是 Account 模型，日常生活中我们碰到的都是 Account 模型。但中本聪在发明比特币时，抛弃了 Account 模型，而是发明了 UTXO 模型，我们不知道中本聪是如何考虑的，但经过分析发现，UTXO 有一些无可比拟的优势，比如，从长远来看，Account 模型的数据库会无限膨胀，但 UTXO 数据库则可以做到最精简，只需保存所有的 UTXO 就能正常使用。此外，UTXO 模型更加有助于实现匿名性，其实对于比特币来说，只有 UTXO，所谓的地址是方便人为记忆的，币都是存在 UTXO 上，用户完全不知道两个 UTXO 背后是不是同一个人。比特币区块头结构为：

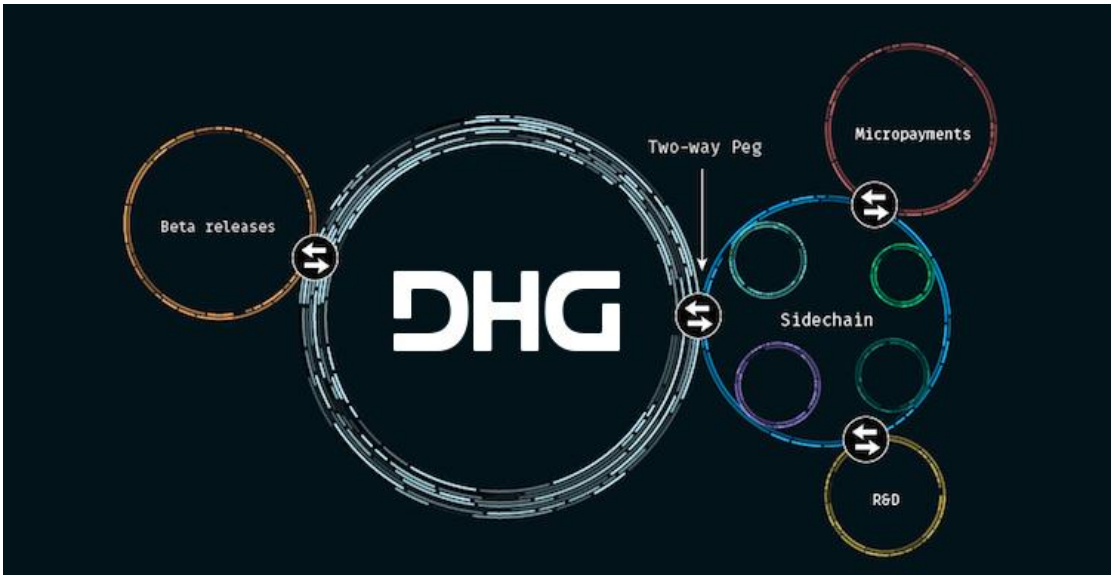
字段	描述	何时更新	字节数
Version	区块版本号	更新软件并制定新版本区块	4
hashPrevBlock	前一个区块哈数值，256 位	新区快产生	32
hashMerkleRoot	交易列表 Merkle 树根，256 位	纳入新的交易	32
Time	区块 Unix 时间戳	每一秒	4
Bits	难度，按照一定规则压缩表示	难度调整之后	4
Nonce	随机数，32 位	尝试新的挖矿结果	4

以太坊采用 Account 模型，为了避免双重支付，需要引入一个递增数（Nonce）作为每一笔交易独一无二的标识。由此带来的影响是，对于同一个 Account 来说，必须是前一笔交易被确认之后，后一笔交易才能够被确认。

DHG 将继承比特币的设计，采用 UTXO 模型。

侧链

侧链是比特币社区于 2015 年提出的非常重要的比特币改进协议，也是实现 DHG 区块链网络技术核心。侧链可以让用户在主链（例如比特币链）与其他具有不同功能的侧链之间相互转移资产。侧链是以锚定比特币为基础的新型区块链，以融合的方式实现加密货币金融生态的目标，而不是像其它加密货币一样排斥现有的主链。用户可以根据自己的需求搭建很多条侧链，所有这些侧链依赖于主链，当侧链的使命完成之后，还可以移除掉侧链，此举可以保障主链的精简特性。侧链本身又可以作为局部主链，以发展其他侧链。

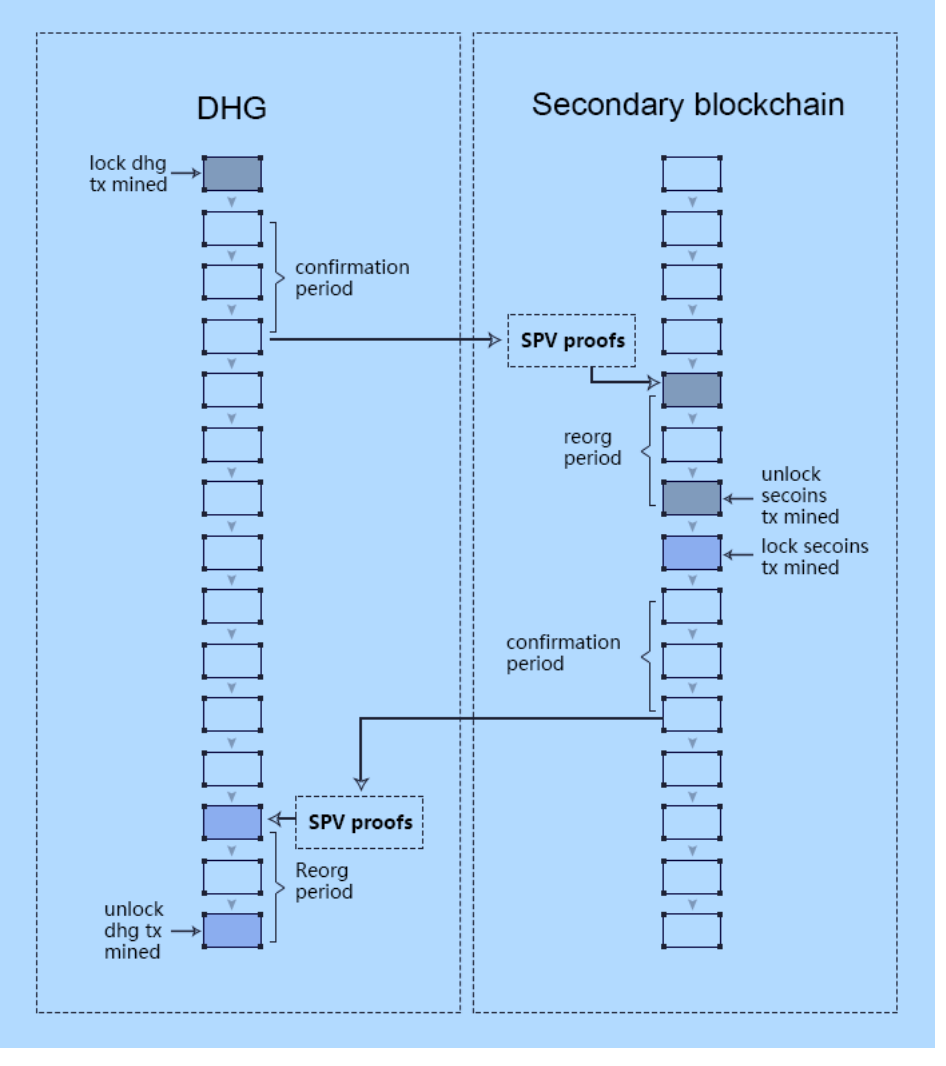


比特币和以太坊只有一条主链，所有功能和数据都加入主链，可想而知，必然的结果是导致区块快速膨胀，超大的区块体积以及超长的同步时间都会让用户痛苦不堪。

DHG 既支持侧链，又能实现智能合约，不过跟比特币和以太坊都不同，DHG 将复杂的智能合约实施为一个侧链，以增加主链网络的价值。

双向挂钩

双向挂钩的想法来源于《侧链白皮书》，是一种可以让比特币在主链和侧链间来回传输的解决方案。然后，所谓的“转移”本质上是不可能发生的，比特币是一套自我完备的系统，通过 UTXO 管理系统内的所有币，不受外界干扰，不可能真的将比特币转移到侧链，侧链上的币也不能真的转到主链。那为啥又说将比特币转移到侧链呢，这其实是一种错觉，所谓的“转移”其实是将比特币暂时锁定在主链上，同时在侧链上释放等值代币。而比特币目前实际上是没法锁住币的，所谓的“锁住”，需要第三方认为介入监管实现。



比特币最大的突破在于，他是真正意义上的分布式自治系统（DAO），如果引入第三方监管，无疑是大大降低了 DAO 性能。其实技术上是可以解决这个问题，只要在比特币现有协议上增加锁币以及解锁触发机制，同时在底层数据做一些扩展，使得主链和侧链存在一些强关联，就可以实现了，不过至少需要比特币发生一次软分叉才能支持。

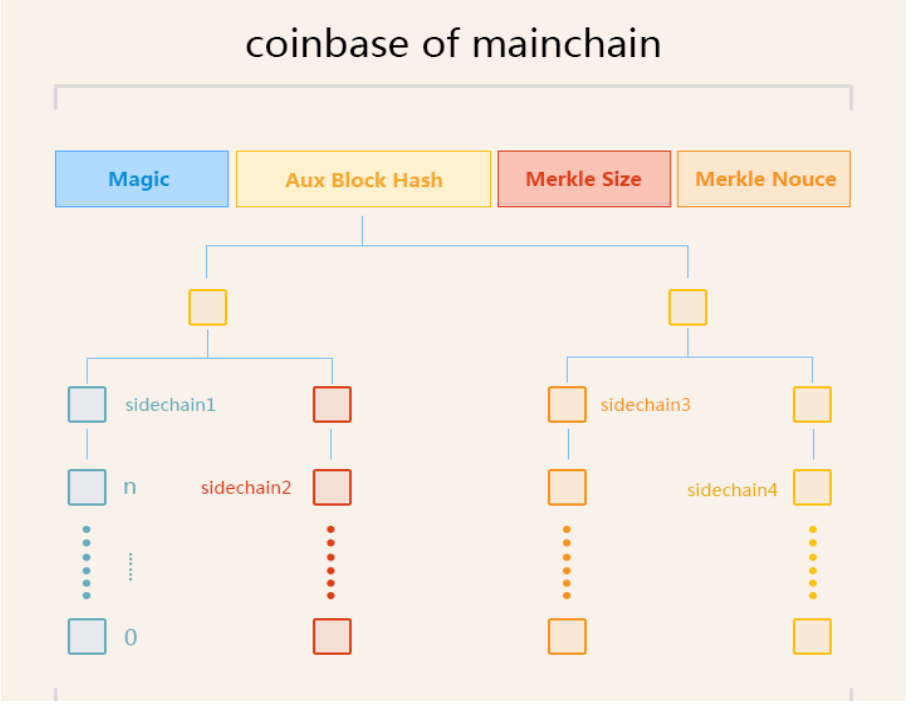
这也是 DHG 的优势，无需担心分叉问题，DHG 启动之初就设计好并实现锁定和解锁机制，即双向挂钩机制。支持侧链是 DHG 协议的一部分。

混合挖矿

侧链的一个核心问题是安全，而区块链的安全主要取决于激励机制，维护侧链对于主链矿工来说是一个额外负担，一个合理的措施是让矿工也获得相应的额外收益。

DHG 采用混合挖矿（Merge-Mining）协议来解决该问题，即矿工在全力维护主链的同时，还能选择性的同时维护侧链，矿工可以同时获得在主链和侧链的收益。混合挖矿是一个成熟的协议，最早用于 Namecon，现在莱特币和狗狗币也采用混合挖矿。使用混合挖矿有很多好处，首先有助于提高系统安全性，因为在主链模型里，我们是在必须相信矿工的前提下应用系统，因此主链矿工被认为是可信的。

采用混合挖矿，侧链的区块哈数值必须要内置于主链区块里，且主链的区块难度必须要符合侧链难度限制。为此，需要对主链和侧链的数据结构有一些相应规定，主链 coinbase 要插入特定格式的数据。



除了混合挖矿，还必须结合 SPV 验证方式，主链不可能保存侧链的所有信息，但可以保存区块头信息，配合交易分支（Branch），就可以实现 SPV 验证，矿工能同时获得主链和侧链的收益。

闪电网络

闪电网络（Lightning Network）起源于比特币的扩容问题，其目的是实现安全地进行链下交易，无需信任对方以及第三方即可实现实时的、海量的交易。在闪电网络出现前，比特币社区为了扩容问题提出很多解决方案，比如硬分叉扩容、隔离见证等，这些技术在一定程度上增加交易处理能力，但其实不能导致交易处理能力得到本质改善。

吞吐量本质上一个受限于底层硬件的问题，包括容量，带宽等，闪电网络则直接跳过区块链，试图在链下实现大量交易，只有必要的时候才会放到链上。闪电网络提供了一个可扩展的微支付通道网络。

如隔离验证一样，比特币至少需要通过软分叉才能支持闪电网络，DHG 直接内置支持，DHG 闪电网络方案可借助主链矿工支持，矿工可作为第三方提供数据存储支持。交易双方可借助矿工开通一条连通双方的、由多个支付通道构成的支付路径，闪电网络可以利用这条支付路径实现资金在双方之间的可靠转移，并实现瞬间到账。

4. DHG 使用场景

这两年区块链发展势头扶摇直上，各行各业的人都在讨论区块链潜在的应用价值，

在金融领域，流通、支付、ICO 等在不断发展。在医疗领域，人们讨论区块链存放病例的巨大优势，在法律领域，区块链在存在证明、智能合约领域拥有很大的应用前景。

数字资产

所有的东西都可以数字化，资产数字化后可量化，可流通，买卖，抵押，催生巨大价值。想象一下未来我们的房子，汽车等都变成了区块链上的资产，私钥决定所有权，如今的不动产届时将具备巨大的流通性。区块链应用于数字资产，最大的优势在于，资产一旦发布到区块链上，其流通不再依赖于发行方，资产变成社会化传播方式。

DHG 将提供多种资产数字化方法，可以通过侧链开通一个应用，并同时发行一种数字资产，也可以通过智能合约构造资产。

数字身份

如今当我们入住酒店，买车票等都提供身份证，其实，我们无需让酒店知道那么多信息，理论上我们只要能证明自己身份清白，有钱支付房费就可以入住酒店了，这是传统身份识别的不足。数字身份很好的解决了这些问题，而基于区块链的数字身份更是具备绝对的不可篡改等特点。

区块链在产品供应链溯源领域同样具备天然的优势，公开的不可篡改的区块链记录，可以清晰的标记产品的流通过程。

DHG 区块网可用于数字身份，食品，药品，工艺品，文物等领域，以证明数据及产品所有权问题。

区块链金融

比特币一开始就被设计为一个金融工具，并且已经在支付领域展现了无可比拟的优势，区块链的优势体现在金融领域的方方面面。比如证券交易，是区块链非常适合的应用领域，传统的证券交易需要经过银行、证券公司和交易所等机构协调结算，效率低，成本高，但区块链系统就可以快速精确的完成这些事情。除了交易环节，区块链在审计方面的优势也很突出，结合智能合约，区块链可以自动完成各类复杂的审计工作。
DHG 打造的区块链网络，有助于各类资产自由流通和兑换，这将是未来区块链在金融应用的基础。

社会治理

在传统领域，身份认证，健康管理，公证，司法仲裁，投票，借贷系统等，使用

中心化服务器存储数据都会存在造假问题。如今全球各地，假证到处都是，要解决这个问题，使用区块链再适合不过。区块链天然的具备公开透明，公平公正不可造假的属性，且成本低，因此我们可以预见，未来所有公证类应用都会选择用区块链技术来解决造假问题。

DHG 的侧链机制将可以对数据进行分级处理，重要的数据放在主链，次要的数据可以放在侧链。

智能合约

IBM 已经研究物联网多年，直到区块链出来，才找到了解决方案，智能合约是真正智能化，自动化的基础，是物联网实现的基石。智能合约的实现使智能社会成为可能。未来人类社会的很多规范，很多合作将由智能合约来完成。

就目前而言，限制区块链应用最大的瓶颈在于速度和容量。速度方面，如今以太坊测试方案已经可以做到 15 秒一个区块，DHG 将紧跟区块链技术发展前沿，优化区块速度。在容量方面，DHG 一开始就解决比特币扩容问题，并且研究分片技术，往无限扩展方面发展。

DHG 的发展目标是做物联网底层协议，为未来可编程社会提供服务。

去中心化应用(DAPP)

在去中心化运算及去中心化数据存储的基础之上，可发展去中心化应用，dapp 也是物联网的发展基础。DHG 最终可提供两种搭建 adpp 的方式，即通过侧链的方式实现，或者通过智能合约的方式实现。通过侧链的方式实现，可不受主链的限制，每一个 DAPP 对应一个侧链，ADPP 可以定义自己的用途及使用周期，即便 ADPP 出现问题，也不会影响到主链，这也是发展侧链的核心意义之一。通过智能合约的方式实现，可共享主链资源。

5. 总结

中本聪发明了比特币之后，虚拟币，区块链行业获得飞速发展，每过几年，整个行业的技术都会迭代一次，目前已经由几年前的对于“币”的探索，转为当前对“区块链”探索主流，下一步，将是往“网”的发展方向，区块链将发展成为物联网的核心技术。

DHG 顺应资产数字化发展潮流，秉承统合综效的设计理念，在保留比特币、区块链核心价值的基础之后，充分吸纳其他区块链项目的创新点，并注重可行性和兼容性原则。

DHG 汇聚当前区块链发展的众多前沿技术，比如侧链，混合挖矿，智能合约平台等，是一个由主链及众多侧链混合交叉的区块网应用平台。

DHG 在数字资产，数据确权，区块链金融，社会治理，DAPP 等领域将发挥重要作用，侧链和智能合约的结合可作为物联网发展基础，甚至是未来可编程社会的发展基础。