GMC

云矿机白皮书 1.0

打造全球 5G+区块链数据确权应用云矿场生态体系

构建一个通用、支撑功能完善、性能高、 应用场景丰富、易于使用、用户体验好公链体系及相关的基础设施，打造 5G 结合数据确权应用的区块链生态系统。

2020

前言

每一次产业变革的浪潮都带给世界全新的机遇与想象。区块链技术的诞生，真正意义上实现了全新的价值转移通道，其应用场景几乎不可限量。区块链技术的优势无疑在数字经济发挥重要作用，创造更大的价值。在新的数字时代就需要更创新的经济模式，区块链技术无疑提供了一种新的可能，真正实现了价值的再发现。人类上百万年的发展历程，一次次重复着这样一个逻辑，就是如何降低人力这种资源被重复使用；从人类发明使用石器，提高劳动效率，到发明使用铁器，到发明使用蒸汽机，到发明使用计算机，再到发明使用人工智能等都在重复这个逻辑。

人作为社会网络中最重要的节点，既是社会网络的缔造者，也是被网络驱使的劳动力，而往往大部分劳动力是被重复使用，没有价值回馈的；或许人类需要一种技术，让解决这个问题成为可能。面对数字经济的变革浪潮，让资源的使用变得更加便捷和高效，但同时有可能造成更大的资源“浪费”，而这种“浪费”是无偿的，没有任何价值回报的，或甚者存在被剥削的可能。传统的社会网络在数字经济网络是否遵循那个人类不变的逻辑，人力资源的价值如何被准确的度量，从而确真，确信，确价和确权成为当务之急，GMC正在进行这场伟大的社会实验！

目录

1. 摘要

区块链技术作为去中心化的价值传输系统，由匿名人士中本聪首次提出并应用到比特币当中。在比特币系统中，为完成相对复杂的交易类型，中本聪创造性的提出了脚本机制。但当开发者想要通过比特币脚本实现更多的功能时，往往就会受到诸多的限制。为此，Vitalik Buterin 提出的 Ethereum 通过引入图灵完备的智能合约和 EVM 使得基于区块链技术的应用开发成为可能，并被业界称赞为继比特币之后的“区块链 2.0”。但无论是比特币还是以太坊，都面临着由于用户与交易增长过快所带来的拓展性及交易延迟的问题。究其根源，在于当前区块链系统中单链的结构，使得诸多优秀项目在这些问题面前都缺乏足够的灵活性，区块链在5G这一天生适用的领域的发展也举步维艰。

为解决这些问题，并更好的将区块链与5G技术相结合，经过不断地探索论证，由美国 GMC 资深技术团队提出了 GMC 树型区块链技术，GMC 呈 “主链+ 多应用支链” 的树状结构，通过支链的无限拓展实现单链结构无法解决的交易拓展性和高并发性问题。同时 GMC 作为5G的基础设施，将建立多实体的设备互信及异构环境下的数据互通，为未来5G更复杂的商业模式打造稳定可靠的技术基础。GMC DAPP 是一款全球领先的去中心化的区块链全领域生态系统，其底层架构技术由来自美国硅谷的顶尖技术团队研发；是您的数字资产分布存储、匿名交易的管

家，更是增值托管、私密聊天、影视娱乐、矿池挖矿、跨境购物、国际STO、创投创业等多为一体的DAPP 应用软件。

2. 全球5G应用发展的现状

通信技术从1G到2G可以说是从模拟到数字的升级，代表着两种通讯网络模式的演进；而从2G到3G，则主要体现在传输速率的明显提升；3G到4G传输速率更快了而且流量资费也有了大幅的下降。总体而言，通讯技术的代际升级，主要体现在通讯速度、传输速率的提升，而通讯速度、传输速率也是制定通讯标准时最主要的参考评价标准，高代际往往伴随着高速率、大带宽、低延迟和高可靠性。5G时代的到来，则主要是这些具体技术指标的实现。5G的主要特性就是超高速、大连接以及低延迟。

2020年是5G的冲刺阶段，各国纷纷加快5G商业化进程。随着5G技术成熟，许多新兴的行业，如智能安防、无人驾驶、VR/AR、智能城市、智能家居等都将得到极大改造，5G将改变我们的生活和工作方式也将引领更多的新兴应用场景和商业模式，未来电子信息技术的诸多创新将主要依赖5G通讯技术，随着5G 标准和频谱生态环境的统一发展，各国加快了5G的商业化进程，在5G技术的发展道路上竞相卡位，竞争激烈。

美国、日本和韩国在2017-2018年部署了5G测试网络，2019年将部署符合5G 国际统一标准的设备。特朗普日前宣布了一系列倡议刺激美国的5G网络发展，特朗普强调称，2019年底前美国将有92个商用5G网络准备就绪，无线通信产业计划在5G网络上投资2750亿美元，可以迅速为

美国创造300万个就业机会， 并为经济注入5000亿美元，苹果正在为推出5G iPhone做准备，台光电、臻鼎KY、台郡三家企业成为首批拿到PCB 订单的厂商。欧盟在2017年开始5G试验，计划到2025年全面部署5G。美国监管部门正在对5G频率进行统筹，3.4-3.8 GHz频段协调进展最快;瑞士有可能成为全球首批推出5G商用服务的国家之一; 爱立信与西班牙电信将著名的诺坎普体育场升级为5G体育场。韩国LG U+已部署1.5万个5G基站，华为设备占95%；三星正进行5G业务并购目标2022年占据20%设备市场份额;韩国电信巨头SK推出5G边缘计算开放平台向第三方开放推进5G商业化。

相关数据预测，5G在应用和消费的推动下，五年左右的时间全球用户将会达到十亿级别，到2035年5G将在全球创造超过12万亿美元的经济产出；预计2020-2025年期间，中国5G商用直接带动的经济总产出超过10万亿元人民币， 间接拉动的经济总产出将超过24万亿元人民币；预计到2025年，5G将直接创造超过300万个就业岗位。

任何商业、任何技术，只有能为用户创造价值，它才是成立的。作为深耕5G技术多年的GMC团队，拥有多项5G专利技术，面对着5G赋能应用的巨大市场， GMC团队始终相信，赋能区块链项目、实体经济是技术发展的必然趋势，将高价值“数据”进行互通是技术发展的必然结果。

美国的测试实验中，GMC团队验证了第5代移动通信传输速度可达10Gbps，比第4代通信网络的传输速度快数十倍至百倍，用户体验速率

达到1Gbps，连接数密度为106万个/km2，空口延时延1ms，端与端时延为ms量级，可靠性接近100%，完全可以现实连续广域覆盖、低功耗宽连接、低时延高可靠的应用场景。

GMC团队成员中也包括比特币社区的技术极客和来自全球各大领域的精英人士，精通区块链、比特币底层、以太坊底层、边缘计算、大数据等技术，以5G 技术赋能区块链项目，在数据安全、身份认证、隐私保护方面将更有优势，在去中心化的节点上确权和分发，促使点对点的价值交换成为可能，组成5G时代下的新互联网基础架构。

着眼于GMC 的应用场景和衍生产品研发，GMC团队专注于开发一系列新的协议和方法来帮助不同项目和资产相互交流，借助5G时代风口，一方面通过矩阵网络架构解决线上及线下应用场景的复杂性，另一方面则可以通过多接入边缘计算的计算能力下沉到边缘节点，提供第三方应用集成，为移动边缘入口的服务创新提供了无限可能。

3. 项目介绍

GMC的目标是由5G工业应用全球联盟发起的一款完全匿名5G应用公链，打造全球5G+区块链数据确权应用生态体系，构建一个通用、支撑功能完善、性能高、 应用场景丰富、易于使用、用户体验好公链体系及相关的基础设施，打造5G结合数据确权应用的区块链生态系统。聚焦5G+区块链数据确权应用和平台层核心技术，构建具备独创完全分布式匿名P2P网络通信协议、独创复合交易分群共识机制和挖矿机制、支持交易匿名保护、图灵完备智能合约等特性。支持第三方资产发行、跨链通信、多链融合等功能，能以公有链、联盟链、私有链等形式落地到实际应用场。

3.1 理念与愿景

愿景是应用5G结合区块链去中心化技术实现数据确权、跨境支付、产品溯源等全方位价值体系的商业化生态应用体现，突破价值传输网络各类关键技术，构建全球价值互联网，为各类价值传输应用提供基础网络。其生态平台将“5G+ 区块链数据确权生态应用” 以新的方式紧密联结在一起，形成一个前所未有的数字世界应用生态。生态链与生态圈之间相互交错、形成矩阵结构，共同构成完整、开放循环的生态系统。

依靠对团队对金融行业深刻的认识和积累，以及对去中心化信仰和自由主义的坚持，将让引领一个资产安全，充分自由的匿名大数据应用时代。

3.2 GMC全球矿机节点

全球矿机节点是运行在p2p网络上的服务器，让小节点使用它们来接受来自全网的动态变化。这些节点需要显著的流量和要消耗大量成本的其它资源，由此在一 段时间内会观察到比特币网络上的这些节点数量呈现稳步下降的趋势，使区块广播的时间需要额外增加 40 秒。为解决这问题，提出了许多方案，GMC团队引入微软研究的新奖励计划和Bitnodes激励计划。

全球型节点：“主节点masternodes” 和 “ 矿工miners”，主节点提供即时发送和私人发送功能，即时发送允许主节点在一秒钟内达成共识，从而产生不可逆转的交易。 “ 私人发送”使用混币技术来掩盖给定交易的发件人和收件人钱包，由于网络是基于工作量的证明，因此还有挖掘节点来计算哈希值，以便加密地保护GMC区块链。为继续发展和营销业务，GMC将支付 “ 区块税” 。GMC依赖于主节点来发送匿名交易，但是这种类型的交易不是必需的。与其他公链不同的是，区块链上可以看到地址和持有量，未使用匿名发送执行的交易可能会被审计。

在节点交易方面，GMC采用混币技术。混币技术基于将交易分组在

一起以创建联合付款的原则。当进行联合支付时，不可能在交易中将输入和输出联系起来，从而阻止第三方确定交易的方向和金额。基于CoinJoin的混币方法增加了所有用户的隐私，因为交易的所有输入不再可能来自单个钱包，因此不再可能与单个用户可靠地关联。从而确保GMC用户私人信息的匿名性与加密性。这些节点对于整个GMC生态的健康而言十分重要，它们能让客户端同步和通过全网快速广播信息。同时，GMC团队同样正在尝试增加次级网络，名为GMC主节点网络。这些节点将具有高可用性，而且在为网络提供符合一定要求的服务后能够得到主节点服务奖励。

现行数字货币网络全节点锐减的主要原因是缺乏对运行节点的奖励。随着时间的推移，全网接入的用户会更多，对带宽的需求会更高，对节点运行者的资金需求也更多，结果使运行全节点的成本提高。考虑到成本的上升，节点运行者必须要降低他们的运行成本或者运行轻客户端，但这样完全不利于整体生态健康。

正如比特币网络一样，主节点是全节点，但不同的是主节点必须对全网提供一 定的服务，并需要一定量的押金才能加入。押金不会丢失，在主节点运行时也是安全的。这可让投资者为全网提供服务的同时，赚取一定的投资收益，减少了价格的波动性。

运行一个主节点，需要存储一定数量的GMC。当主节点生效时，它可为全网的 客户端提供服务，并以利息的形式获取奖励。这就使得用户为这项服务投资， 但同时得到一定的回报。主节点获取的收益是来自同

一个矿池，大约有45%的 区块奖励纳入到这个计划中。考虑到主节点奖励计划的奖励率是固定的百分比，还有主节点网络节点存在波动的事实，预计主节点奖励会根据当前生效的主节点总数作出变化。

4. GMC生态应用介绍

GMC 是构建于 P2P 网络的区块系统，同目前流行的 P2P 数字货币系统类似， 以去中心化方式维护透明账本，实现用户数字资产自主安全管理和高效流动。GMC 系统针对5G+数据业务需求设计，利用区块技术为 数据业务提供去中心化安全管理平台，实现系统所需高并发低延迟等性能要求。

GMC 通过安全共识组织用户交易（transaction），按时间顺序形成数据区块。同 Bitcoin 等单链系统不同，GMC 采用树结构来存储排列区块，可以根据业务类型和数据负载进行分叉形成多个分支。分支之间区块相互独立，新增区块只与自身分支数据相关。在多重分支的情况下，根据业务数据流量，可以分布到多个分支区块中，由此产生的可扩展性和高并发性正是 统所需的基本性能。GMC 的多重分支结构由唯一安全主链和众多应用支链构成，安全主链用于支撑全网共识机制，应用支链用于实际业务。在应用支链可以提供最低 2 秒的低延迟交易确认，用户可以指定交易紧迫性，支付相应交易手续费， 以此实现低延迟业务。

4.1 GMC数据确权——自由化资产管理

随着数字货币被逐渐进入大众视野，数字资产开始逐渐被投资者接受。然而由 于区块链技术相对极客，资产品种快速增加，投资资产筛选难度高，投资渠道相对分散，对普通投资者来说门槛较高。专业的资产管理服务必将是未来的趋势。GMC将推出基于区块链数据确权应用的资产管理服务平台GMC，降低数字资产的投资门槛、交易和管理成本。目前，公司已经完成组合分析工具的研发，并开启测试。

GMC希望用区块链技术、工具产品解决传统资产管理暴露出的诸多问题。GMC 团队计划开发研发和开源用于数字资产投资托管的智能合约，规范投资顾问和出资人的行为，实现委托、行为的安全、透明，建立资产管理平台，并从中获得相关收益。团队计划将于2020年完成并上线相关功能。

团队对产品的未来发展相对乐观。传统的资管服务平台往往会收取相对较高的管理费和业绩分红，通过区块链去中心化的技术，仅将委托规范放入智能合约，可以降低管理费用，降低交易成本。

要用互联网的方式做资产管理平台，必须要聚集出资人和投资顾问。为此，团队前期将推出数字资产组合分析工具、智能交易工具，通过解决目前投资人的痛点，以聚集一部分潜在出资人，并筛选出一部分投资收益率较高的用户作为未来潜在的投资顾问。

目前，团队已经研发完成了数字资产组合分析工具，用户只需要填

写各交易平台账号，可以在平台上实时查看自己在各个平台的资产价值及收益率，同时获知投资的潜在风险。针对目前交易平台分散的问题，团队也正在研发智能下单交易工具，计划于2020年下半年推出，以帮助用户在一个平台上完成各平台的交易，以此增加平台用户的粘性。

4.2 GMC跨链电商交易

GMC 跨链模板和电商模板的实现方式，由于无需 VM 编译，所以相较智能合约和脚本来说，模板的运行效率非常高。同时 GMC 交易运行速度快、安全， 没有 VM 一样的可被攻击的漏洞，防止因为 VM 漏洞导致链上代币被盗或归零。但是非智能合约，版本更新过程稍显麻烦，程序发布后，需要同步更新到每个客户端，后期会增加模板自动更新模块。

4.3 分布式账本系统

面对着当前区块链账本方面存在的问题，GMC团队同样致力于研发全新的账本系统，以推进区块链行业的持续发展。目前，研发出的GMC账本已经处于上线前的内测阶段。GMC账本首先是一个分布式账本，交易总账是存储于系统参与者各自的服务器上。这就使得市场中的一部分不完全信息博弈将变成完全信息博弈，没有任一方可以随意篡改账本，监管机构将可以根据总账进行审计。从更高级的层面来说，可以打通各个金融机构之间的壁垒，使得账本互通，所有金融机构使用同一个账本。这就使得离柜市场和场内交易的边界将变得模糊。 运营数据分析将会更加高效可靠。

在GMC账本中，每一个节点并不是像比特币那样保存账本的完整副本，节点只能看到网络中与自己相关的交易。具体地说，节点能看到自己直接涉及的交易，以及需要验证这些交易的前置交易。从而保证了交易的匿名性和加密性。

当GMC节点处理交易时，它必须下载并验证该交易的所有祖先。因此，如果交易流程长，新的交易可能需要验证大量的祖先，从而触发GMC的可伸缩性问题。 此外，如果交易包含高度杂交，则新交易的祖先可能包括网络中的许多或大多数过去的交易。

相比之下，如果交易的历史很“浅”，并且包含许多不相互影响的断开的交易链，GMC的优势就十分明显。节点永远不需要同时验证大量

交易，并且可以对与其自身无关的大多数交易保持沉默。如果用作财务分类账，可以说GMC 非常适合高度分散的市场，其资产很少易手。

公证人机制是GMC网络交易验证和确认的核心机制，这个机制避免了交易信息在全网广播，这主要是为了支撑交易信息“ 适度可见” 的能力。另一个目的是将共识机制与交易流程分开，变成一种标准服务，从而可以采用不同形态的 共识实现方式，而非绑定到某种特定算法上。

公证人是有一个独立的、交易双方（ 多方） 都信任的角色，可以确认交易的有效性。交易的有效性是指某项输入数据没有曾经或正在成为其他交易的输入。 从这个角度讲，公证人机制就是比特币的共识机制——区块链—— 的替代物。GMC账本并不是一个开放式的网络，而是一个半信任的网络，参与方和节点的 加入都是可以事先经过审核的，这就很大程度上降低了攻击发生的概率。即使 存在恶意攻击，参与方也需要付出声誉的成本和相应的法律风险，这跟比特币这种完全开放式的匿名网络是完全不同的。

4.4分布式社交网络应用

分布式社交网络应用基于区块链技术与分布式P2P技术，实现一个去中心化， 可任意访问，不受任何组织影响的社交网络世界。不同于日常访问的社交网络， 分布式社交网络没有服务器的概念，所有网络数据都被分数在分布式社交网络各个用户的电脑中，任何人都只需要一对基于

GMC的非对称密钥，就能够发布内容。

所有人都可以通过发布者公布出的站点私钥在P2P网络中找到发布者的电脑，直接从中下载站点的数据。越来越多用户访问后，发布者的内容就会被多台电脑保存，曾经访问过用户社交主页的电脑就会开始为用户的站点做种子，就像BT种子一样，用户的站点的内容就这样在无数台电脑中存续，会被永久性存储。 同样，GMC分布式社交网络由于P 2P无中心化主机特性，建立网站也变得非常的简单，不需要去租用主机，用户需要的仅仅是通过命令生成一个随机网站地址，写好它的HTML代码，然后发布给其他人。

4.5 GMC 5G矿机矿池

GMC 提供5G矿机租赁和订购，增加用户多元化的投资方式。抛开高风险的炒币者，适合长期看好主流货币的价值投资者，平台会提供全球高性能低费用的矿场进行托管挖矿，适当的收取部分托管费用，持有 GMC可以通过在线租赁和直接订购矿机以及支付托管费。

持有 GMC 的5G生态系统通证，通过 5G矿机挖矿获得收益,持有GMC 越多获得收益也越多。GMC通过社区有效节点激励方式，让更多的系统用户成为社区节点一员，达成共识推动整个生态系统的快速发展，随着各个场景的落地应用，GMC 的价值也逐步上

升。

4.6 GMC娱乐应用

GMC 娱乐直播平台，可互动娱乐，可本人自娱自乐，可用 GMC 打赏。为用户提供了区别于以往录播的实时直播内容，实时观看、深度互动的体验给用户开启了一个新的大门。应用5G技术，提高娱乐体验感；同时，正因为用户可以用“GMC”的盈利模式得以建立并发扬光大，成为继“游戏、广告、电商”以外的第四种互联网盈利方式。

4.7 GMC智能量化交易

GMC的AI 智能高频交易和搬砖套利，提供用户更多的增值渠道，专业团队打理，省心省事。GMC 可以 24 小时监视行情的变化，在全球各大交易所进行高频交易，GMC AI 会根据您的设定，自动进行低买高卖。智能化全自动交易 APP 一键托管和搬砖套利，托管费须 GMC支付。

5.树状区块架构

在如今常见的区块链项目中，所有交易信息均存储在单链区块当中，使得整个系统面对不断增长的交易规模时缺乏足够的灵活性。在GMC 中，主链数据与应用数据进行了分割处理，以“安全主链 + 多重应用支链”的树状区块结构来存储系统区块数据。

安全主链主要存储交易与安全共识相关数据；应用方则通过从任意链条进行分叉，生成支链（分叉链），专门组织和存储与应用业务相关的数据。 并且随着交易规模的扩大，支链可以继续建立子级支链。通过这种类似垂直分割的方式，杜绝了传统单链结构中所有交易填充在主链区块的弊端， 实现了整体系统的横向拓展。

GMC 上的支链数量越多，系统可承载的 TPS（Transaction Per Second）也就更高，在应用支链足够多的情况下，GMC 整体可实现千万甚至亿级的 TPS 承载。

共识机制简述

众所周知，在“不可能三角”的各种研讨中，去中心的结果往往意味着低效的TPS，而物联网的海量数据就成为共识构建中一块无法搬走的巨石，那么在区块链+5G技术的领域里，究竟什么才会是适合的共识

呢，让我们先从共识算法的演进说起。

Proof of X 是目前公链领域内应用较多的一类共识。其中 PoW 最早被应用， 但存在资源浪费、算力集中、缺少终局性以及性能低下等。

PoS 是目前有力竞争者，可避免资源浪费、弱化了中心矿池需求、降低51%攻击可能性，但也同时存在确定记账节点数量困难、存在非预期的中心化问题、Nothing at Stake 等问题。

为了解决以上弊端，当前也诞生了许多混合类共识，希望既融合两者的优势， 又能规避某些弊端，包括PoW+PoS、DPoS+BFT 等。所以混合共识机制可能会是公链后期发展的一个出路。

PoW 共识算法

PoW（Proof of Work）即工作量证明，根据矿工的工作量对数字货币进行分配，矿机的性能越高，数量越多，工作量越大，得到的数字货币就会越多。

BTC 是采用 PoW 方案最典型的原型。它通过挖掘过程包括解决一个数学问题，矿工通过这种技术手段完成了 PoW，就获得了记账权。因为它需要计算力的资源，成功的矿工会得到 BTC 作为奖励。为了控制货币基础， 挖矿被设置成了更加复杂的模式。因为每个矿工解决问题的可能性依赖于他的算力，挖矿的难度由系统中所有算力的总和来决定。

对于 PoW 机制的加密货币，矿工是通过竞争解决数学问题来确认和固定转账。第一个解决问题的矿工得到奖励。该问题的复杂是刻意制造

的，用来控制货币基础。这个处理过程被一些人认为是天才之举，很好的解决了拜占庭将军问题。但是被另外一些人批评没有效率因为白白损失了资源。同时，单一的 PoW 机制也面临着 51%算力攻击等安全性问题。随着 BTC 的发展与区块链的行业发展，PoW 机制的缺点也暴露了出来。持币者无法参与任何决策，话语权集中在矿工的手中，这与去中心化的理念背道而驰，决策权集中在少数矿工手中。

DPoS 共识算法

DPoS 是基于 PoW 及 PoS 的基础上，出现的一种新型的保障数字货币网络 安全的共识算法。它既能解决 PoW 在挖矿过程中产生的大量能源过耗的问题， 也能避免 PoS 权益分配下可能产生的“信任天平”偏颇的问题。那么，DPoS 就能顺理成章成为共识机制 3.0 脱颖而出的代表性共识机制。 DPoS 它能够让用户广泛参与到挖矿中来 ， 指的是让每一个持币者都可以进行投票，由此产生一定数量的代表 ,或者理解为一定数量的节点或矿池， 他们彼此之间的权利是完全相等的。持币者可以随时通过投票更换这些代表，以维系链上系统的 “长久纯洁性”。

网络描述

GMC 网络由运行 GMC 软件的节点构成 P2P 网络。GMC 的整体网络架构可分为三层：节点网络层、终端服务层、5G终端层。

节点网络层由运行 GMC 核心节点程序的节点构成，节点之间同步校验区块和交易数据，并进行共识组织区块数据。

终端服务网形成分布式终端后台，为 5G终端提供接入服务。

为了支撑庞大的 5G业务，节点网络与终端服务网共同组成 GMC 服务平台。

5G终端层包括智能传感器、控制器和移动终端，内嵌轻客户端程序，本地保存私钥完成交易构建和校验。

系统软件组成

为更好支持5G复杂环境下的多种应用场景，同时保证区块链服务的可靠运行和普通用户的使用需求。GMC 系统软件的设计总体包括五部分：核心钱包程序、轻钱包后台服务系统、移动端轻钱包程序、嵌入式系统轻钱包 SDK 和在线区块浏览器。

核心钱包程序

核心钱包程序用于主干网络节点和普通用户，对运行环境和硬件有一定要求，可以完整使用区块系统所有功能模块。

轻钱包后台服务系统

LWS 是 light wallet service 的缩写，是架设在 GMC 公有区块链主

干网络和终端数据采集传感器设备之间的一座桥梁。通过它，GMC 核心钱包的区块和交易数据及时地更新和缓存在 LWS 自有的高速内存数据库及本地数据库中。

根据这些数据，它会计算出不同终端设备持有密钥所对应的公钥地址的最新UTXO 集合，并通过与 AWS 的5G Core 的 mqtt 连接，将这些信息发布（publish）到亚马逊云端设施上， 由其 message broker 向对应的订阅（subscribe）了这些信息的终端设备转发。相应地，终端设备会根据这些与自己相关的 UTXO 列表，在获取了监控监测采集的数据后打包这些数据到交易中，通过 mqtt 发布到5G Core。

经由后者的 message broker 向订阅了这些设备的发送交易主题的 LWS 推送，LWS 会校验这些交易，如果验证成功，则会通过 Socket API 向 GMC 核心钱包转发这部分交易，后者收到之后通过 P2P 网络接口向 GMC 全网广播这些交易，出块节点收集这些交易，最终完成其打包区块上链的操作。

LWS 使用 AWS 提供的基于长连接、双向的消息 pub/sub 消息代理解除与巨量连接的 device 端数据交互的耦合关系，解决了设备的高并发性和高扩展性。对于区块及交易数据的存储查询及 UTXO 数据的更新，LWS 使用 AWS 的 Amazon DynamoDB 服务存储它们 KV 键值对数据。

考虑到 GMC 公链网络多支链上高并发 TPS 产生的海量交易数据及打包区块数据，以及海量的 UTXO 数据，利用 AWS 的 ms 级响应延迟

的数据存储服务 Amazon DynamoDB，可以为每个业务分支链创建一个区块数据库和交易数据库，加速数据的检索能力。

LWS 同步主干网络下行的区块链数据的同时，配合高吞吐量、弹性扩展的Amazon Kinesis 服务，使用 Amazon S3 高度扩展（Scalability）、高持久性（Durability）和高可用（Availability）的分布式数据存储服务缓存巨量的区块文件到亚马逊云端，完成区块实时数据收集和处理，可以为本地物理地址近邻的其它 LWS 使用，甚至向世界范围的 LWS 提供检索服务， 另一方面， LWS 在与核心钱包失步或数据错误时，可以使用 S3 中的数据快速恢复。此外，LWS 使用 AWS 的规则引擎 rules engine 将消息转换并路由到 AWS 服务，后端使用 Kinesis 服务分流数据到不同的 AWS 服务，或者接驳Lambda 服务分流数据。在区域网络传输不均衡的环境中，也可以使用 AWS 的 CloudFront 服务提供 CDN 类似的功能。

使用 PB 级的 Amazon Redshift 关系型数据仓库，可以存储结构化区块链数据，便于 GMC 区块链 web 浏览器、智能设备钱包 app、GMC区块链开发测试人员调试跟踪程序运行时的数据视图。

LWS 使用高并发语言 golang 开发，程序采用 goroutine 及 channel 设施保证了数量庞大的 device 端同时发送的发送交易到核心钱包主干网络的请求能够及时有效地处理，从而实现了海量交易的高速上链。

移动端轻钱包程序

移动端轻钱包程序可以使终端节点在不运行完整钱包程序的情况下，也能够对交易进行校验。主要用于 IOS 和 Android 移动终端，在网络带宽和硬件性能都有较大限制的情况下，为用户提供安全钱包服务。

嵌入式系统轻钱包

嵌入式系统轻钱包 SDK 为 5G智能硬件提供轻钱包 API，可以通过终端服务器接入 GMC 网络，不需要在本地进行繁重的区块同步和区块数据存储，专注与业务相关的交易数据构造和鉴权。

在线区块链浏览器

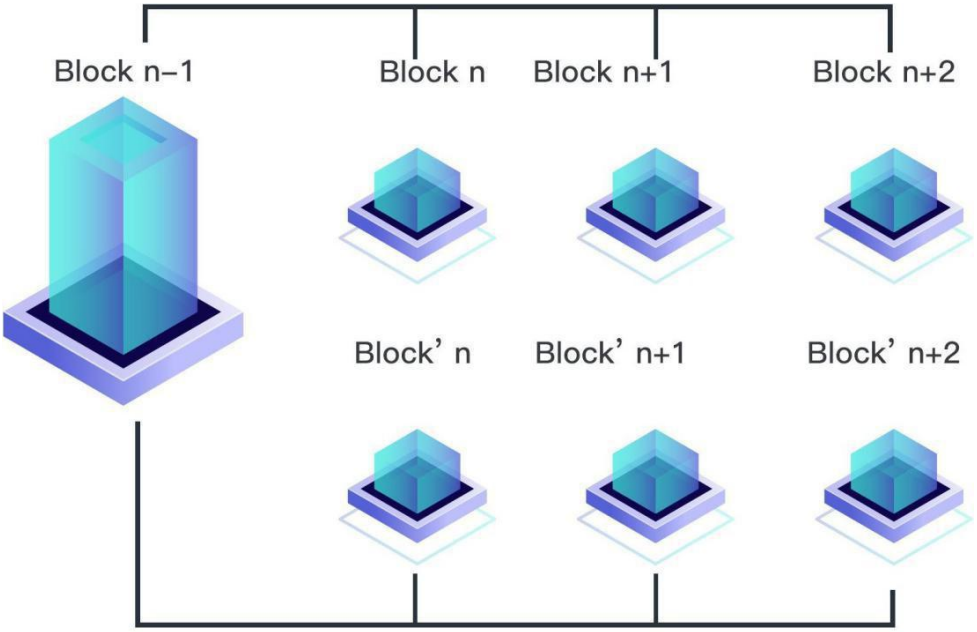
在线区块浏览器配合钱包节点实时展现区块系统状态，查询历史区块交易数据。

分支标识

GMC 系统的区块按时间顺序连接在一起，以多分支形成树状结构。在 GMC 中，安全主链和应用支链统称为“分支”。每一条分支均会有一个独特发的分支标识来进行标记。 安全主链以创世区块 hash 作为支链ID，应用支链以分叉点后第一个区块的 hash 作为支链 ID。

在分叉之前，父链和支链拥有完全一致的链结构和交易；分叉点之

后则相互独立，互不干扰。出现在分叉点前的同一笔 Token 在分叉点之后可以在父链及支链中创建不同的交易发送到不同的地址；分叉点之前的区块数据在父链及支链中也可以通用。 用户在创建交易的时候需要指定一个锚定区块，标定在此区块之后的所有 支链有效。如果锚定区块设定为 Block n-1, 创建的交易会被包含到两个支链中；如果设定为 Block n，则该交易只在父链有效，支链中可以创建新交易将 Token 发送其它地址。



安全主链

安全主链为 GMC 树状结构中的主链，所有的支链均为其“后代”，其被用于支撑全区块系统的安全和共识，在 P2P 网络中主链的同步广播消息转发优先级高于应用支链。安全主链除了记录主链 Token 转移，还保留DPoS 节点协商关键过程数据。安全主链的区块之间不能插入子块， 只能按照既定出块间隔增长。由于会有相当部分容量记录共识协

商过程数据（以 23 个DPoS 节点为例，协商数据会占据每区块 115KB 左右的容量），故安全主链的交易容量低于应用支链。 安全主链以区块系统创世区块为起点， 通过DPoS+PoW 共识顺序产生区块。安全主链被用于支撑全区块系统的安全和共识，所有应用分支节点都需要同步和校验主链区块头信息。新节点接入网络后，首先完成主链同步，才开始进行对应应用分支同步。

主链特殊交易

在安全主链中，鉴于功能特殊性，有三类与共识机制相关交易是安全主链独有的：DPoS 节点投票交易；DPoS 节点登记交易；PoW 出块奖励交易。

DPoS 节点投票交易

DPoS 节点产生一个 Delegate 模板地址，首次需要自己发送Token到该地址，完成 Delegate 地址链上发布；用户使用与 DPoS 节点相同的参数创建Delegate 地址，并将 Token 寄存于该 Delegate 地址，完成 Token 投票。DPoS 节点可以使用 Delegate 地址的投票作为权重参与 DPoS 协商过程。 用户将币寄存 Delegate 地址进行投票时，所有权依然属于用户，并且可以随时取出，但是一旦取出，相应节点的投票数量也随之相减。

DPoS 节点登记交易

DPoS 节点在每轮协商需要筹集足够 Token 投票，并以此创建登记交易提前在链上进行登记和发布自己初始协商参数，只有协商轮次开始前完成登记的 节点（超过总票数的 2%）才允许进入协商过程以及获取出块权。

PoW 出块奖励交易

PoW 共识缺省情况下只用于主链共识出块，对应出块奖励通过这类交易提供给参与者。该类交易的作用类似 Bitcoin 中 coinbase 交易。

应用支链

在 GMC 中，应用方通过在父链发送一种特殊类型的交易 -----分叉交易，用于创建应用支链。应用支链的区块产生间隔需要和安全主链一致，其它主要参数可以在创建分支初始化过程中由创建者配置，可配置参数包括 Token 总量和分布、出块奖励和增发方式等。

新创建支链的第一个区块（分支起始块）被保存在分叉交易中。支链的Token 分布可由创建者定义，有三种方式：

- 创建独立分支，分支起始块重新设置 Token 总数和分配方式；
- 完整继承分叉点 Token 分布；

- 继承分叉点 Token 分布，并在此基础上进行增发，增发部分的分布方式在分支起始块中定义。

自分叉点之后，支链 Token 和父链是完全隔离的。

抵押机制

为了防止恶意人员通过高频分叉对父链带来的资源损耗，每一次建立支链都需要使用父链 Token 进行抵押，分叉交易中用于抵押的 Token 被发送到一个特殊地址进行冻结。抵押 Token 根据父链区块高度和父链区块起始高度差值分阶段解冻，创建者使用自己私钥进行签名后可以将解冻部分 Token 转移到其它地址。创建支链所需抵押 Token 随区块高度和起始高度差值递减，每隔525600 区块完成一次减半。其中抵押 Token 的基数 N 由父链的初始Token 供应总量决定。

6. 用户密钥与地址

GMC 的地址有两类：公钥地址以及模板地址，分别对应特定公钥和模板。地址长度固定为 33 字节，在交互性界面中，采用编码后的地址作为输入 / 输出参数。

```
pubkey address:
encoded address = '1' + BASE32Encode(pubkey + CRC24q(pubkey))
template address:
encoded address = '2' + BASE32Encode(template ID + CRC24q(template ID))
```

其中 BASE32Encode 采用 Crockford 方案字符集， 但不进行该方案中 symbols check 过程。

密钥和公钥地址

GMC 系统采用 curve25519 作为基本安全算法，用户私钥和公钥均为 32 字节，私钥签名为 64 字节。curve25519 安全性和 P256 相同，同安全性算法中是目前效率最高的非对称安全算法。以类型前缀 + 公钥作为钱包公钥地址。

为了保证用户私钥安全，在本地存储采用 chacha20+poly1305 算法加密， 需要用户输入密码才可以使用私钥进行签名操作。

模板地址

模板地址由类型前缀 + 模板 ID 构成。模板 ID 由 2 字节模板类型 + 参数Hash 低位 30 字节构成。例如一个 3-5 多重签名模板：

```
public keys:
  1: fcd74aa82a1eb098830a2fcc877735a60152b441c16b2212157c4215db074e88
  2: f1a1ced60a7ecdf83735a3380765f2ef77221f367da05bd901e885b9d799aec5
  3: c2885254a2acefaeb05bd94b0e73e483bded994b02ebd0bc6b3523c2dde558dd
  4: e2de897ad0935bbfd6cca48da2ee285c87ae784285df35513180143ec55c8450
  5: b1f1ce918f30b46aa3d2648810f6153410e44122c042998699323b982664a16f
tempate ID:
000244c03d536e6175912b3040aa876388b197c21ae55c283f182403ab610852
encoded address:
2a8463ar34gc3ya2wwmdc55xhh1hrfaj060ns2xb1ds9kvg240803k041
```

带参数模板

时下流行的区块链系统可以提供运行于不同 VM（Virtual Machine，虚拟机） 之上的脚本或智能合约，可以对区块系统基本账本进行强大灵活的功能扩展。但是截至目前看来，区块系统中的 VM 模块还处于起步阶段，除了存在内在安全漏洞等问题外，运行效率和使用费率也在一定程度上限制了智能合约适用范围。GMC 系统不提供脚本和智能合约系统，而是采用带参数过程模板实现常用的脚本和智能合约功能。采用对应模板地址为用户提供功能调用。

7.区块与交易

区块

GMC 区块的数据结构设计如下：

Elem	Type	备注
nVersion	uint16	版本号
nType	uint16	区块类型，用于区分创世纪块、主链区块、支链区块和支链子块
nTimeStamp	uint32	时间戳
hashPrev	uint256	前一区块 hash
hashMerkle	uint256	vtx 所包含 transaction 构建的 Merkle Tree Root
vchProof	vector<uint8>	用于校验共识合法性数据
txMint	CTransaction	出块奖励交易
vtx	vector < CTransaction >	当前区块包含交易列表
vchSig	vector<uint8>	区块签名

说明：

- 目前区块版本为 0x0001 。
- 时间戳采用 UTC 以秒为单位。

vchProof 包括了合法性证明系列化数据，在安全主链中，包括 DPoS 节点广播的计算结果（包括各节点签名），PoW 区块中还包括工作量证明参数；在应用支链中，包含同高度主链区块 hash 和共识计算结果。

txMint 不进行签名，签名字段为空。

区块签名 vchSig 使用 txMint 输出地址进行签名，签名数据段包含除 vchSig 以外所有字段。

交易

GMC 采用 UTXO 模型记录交易，包括以下数据：

Elem	Type	说明
nVersion	uint16	版本号
nType	uint16	类型，区分普通交易、投票交易、挖矿
nLockUntil	uint32	交易冻结至高度为 nLockUntil 区块
hashAnchor	uint256	交易有效起始区块 HASH
vInput	vector<CTxIn>	前序交易输出列表，包含前序交易 ID 和输出点序号
addrTo	CDestination	输出地址
nAmount	int64	输出金额
nTxFee	int64	网络交易费
vchData	vector<uint8>	交易数据
vchSig	vector<uint8>	交易签名，可以包含模板参数

说明：

- 目前交易版本为 0x0001。
- hashAnchor 用于指明当前交易起始有效区块以及对应分支。
- 输入列表中的前序交易要求输出地址相同。
- 交易包括两项输出，一项为表中所列（addrTo/nAmount），另

外一项是隐含的找零输出，地址同输入地址，金额为（Total Input - nAmount- nTxFee）。

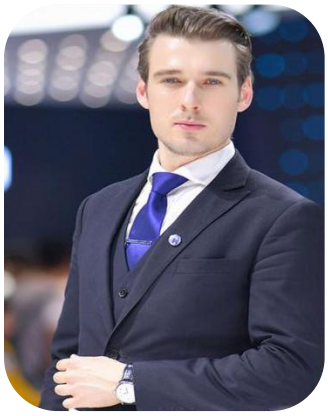
- 交易签名用输入列表统一地址，签名数据段包含除 vchSig 以外所有字段。

GMC 跨分支交易

跨分支交易可以用于实现 GMC 分支之间无信任情形下同步价值交换。实际应用中，往往可以将业务按照业务流程、设备种类、空间地域等关联因素进行划分，分散到多个分支中。互动频繁的设备通常持有同一分支Token，在同一分支进行数据交易。但作为一个业务整体，和持有其它分支 Token 设备交互的需求也是客观存在的。这种情形下，跨分支交易就可以实现支链之间的 Token 交换。一方面跨分支交易可以在无信任情形完成，利用技术原理保证了对双方的公平性；另一方面跨分支交易在两个支链之间同步进入区块，保证了高效率和有效性。这为包括去中心化交易所、Token 兑换网关等应用提供了良好的底层技术支撑。

8. GMC 团队介绍

首席执行官，Peter：菲利普·帕特里克，PCA 区块链实验室联合创始人，区块链资深投资人。留学英国牛津大学计算机科学学院攻读研究生,6 年区块链从业经历，曾带领多只团队从事区块链行业并作为多个区块链项目指导顾问。是最早参与美国 TWITTE 技术程序组管理高层， 在区块链技术的未来的导向上有着独到的见解，并为区块链在价值领域的发展做出了独有的贡献。



首席运营官，Job：毕业于杜伦大学商学院，拥有 6 年金融与财富行业的运营和管理经验，对区块链项目应用发展有着较深的研究，曾是 Ask 公司的运营总监。曾担任 FST 集团，担任瑞典分公司的总经理职务，负责统筹和管理公司

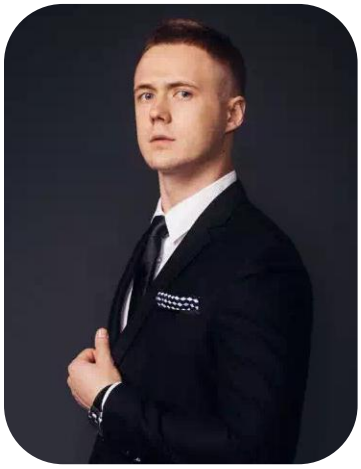
所有事务。创造出连续 2 年的业绩欧洲地区第一。

首席财务官，Alina：毕业于美国斯坦福大学商学院。曾在伦敦任职于汇丰投资银行部，参与过多项投融资项目和筹资交易。曾担任摩根财团非洲地区的投资银行和资产管理公司的财务总监，在区块链领域资产管理和风控管理拥有丰富的经验。至今已有 7 年的高层管理工作经验，在业界有着深厚的人脉，有着深厚的理财与企业风险管理知识。

首席营销官，William：威廉·西奥多，在环球投资和瑞士信贷的技术和银行业务背景下的职业投资经理人，后担任科勒资本的美洲地区风控总监。他在投资机构，风险投资基金和投资者建立足够的信任和影响力。是著名的职业投资人。2013 年，关注区块链行业，并对多个区块链项目进行投资，特别对区

块链底层技术公有链项目发展。现是GMC的主要投资人之一。

首席技术官，Works：沃克斯，毕业于美国耶鲁大学计算机科学专业，作为顶级的 IT 工程师，曾在微软担任澳洲地区技术总监。后又服务于多个区块链团队，有着十分出色的代码和架构技术。并参与多个区块链项目的策划，有着丰富的区块链开发经验。



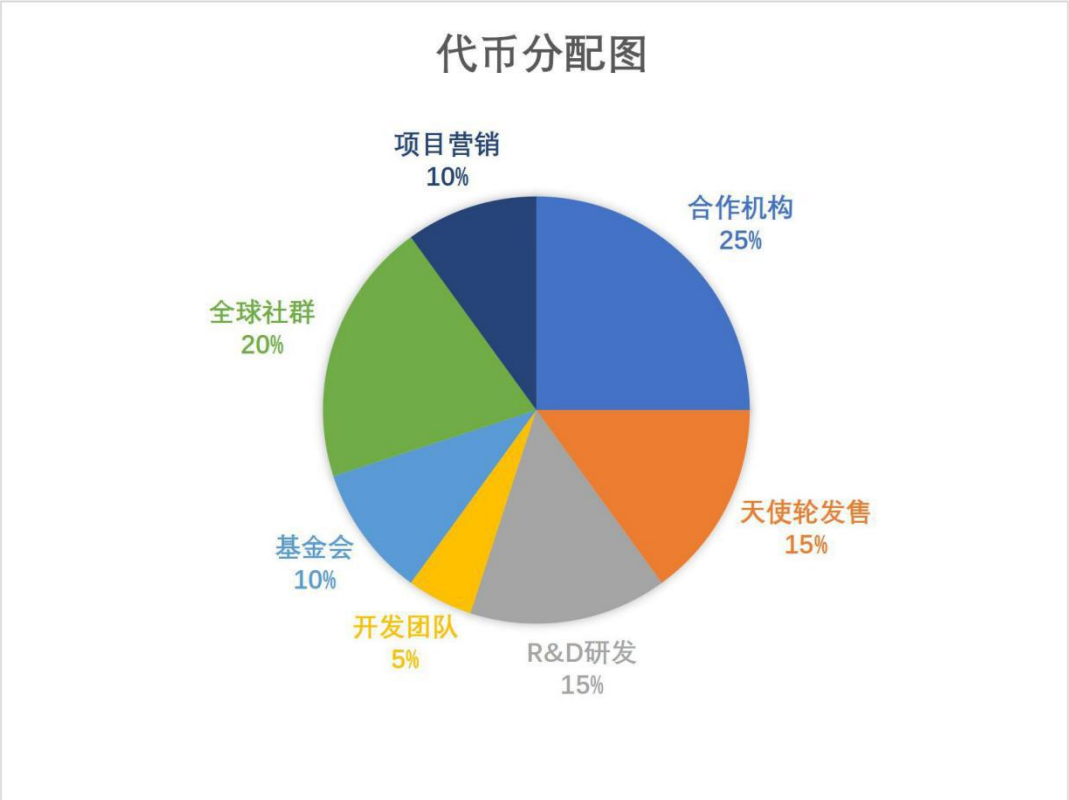
首席战略顾问，Woodrow Dean：迪恩·伍德洛，英国在 IT/媒体、房地产、并购的 FinTech 和 BF 投资等多个行业的跨国投资公司任职，拥有国际税务和法律方面具有丰富的经验。他是多家公司董事会的首席律师。现担任GMC的法律团队负责人。

9. GMC Token分配机制

为了从激励层面推进 GMC生态的发展，GMC恒定发行8000万枚通证，是基于以太坊发行的去中心化数字资产，代币简称:GMC。

代币发行方：GMC基金会。

GMC通证分配比例如下：



10. 免责条例与风险说明

免责说明

除本白皮书所明确载明的之外，GMC开发方不对GMC作任何陈述或保证（尤其是对其适销性和特定功能）。任何人参与GMC项目均基于其自己本身对GMC的知识和本白皮书的信息。GMC开发方在此明确不予承认和拒绝承担下述责任：

1、任何人在参与GMC项目时违反了任何国家的反洗钱、反恐怖主义融资或其他监管要求；

2、任何人在参与GMC项目时违反了本白皮书所施加的要求或义务，以及由此导致的无法付款或无法提取GMC币；

3、GMC的开发失败或被放弃，以及因此导致的无法交付GMC币；

4、GMC开发的推迟或延期，以及因此导致的无法达成事先披露的日程；

5、GMC源代码的错误、瑕疵、缺陷或其他问题；

6、GMC或GMC币未能实现任何特定功能或不适合任何特定用途；

7、未能及时且完整的披露关于GMC开发的信息；

8、任何参与者泄露、丢失或损毁了数字加密货币或代币的钱包私钥（尤其是其使用的GMC币钱包的私钥）；

9、GMC币的第三方众筹平台的违约、违规、侵权、崩溃、瘫痪、服务终止或暂停、欺诈、误操作、不当行为、失误、疏忽、破产、清算、解散或歇业；

10、任何人与第三方众筹平台之间的约定内容与本白皮书内容存在差异、冲突或矛盾；

11、任何人对GMC的交易或投机行为；

12、GMC币在任何交易所的上市或退市；

13、GMC币被任何政府、准政府机构、主管当局或公共机构归类为或视为是一种货币、证券、商业票据、流通票据、投资品或其他事物，以至于受到禁止、监管或法律限制；

资金的安全和管理

项目收到的资金应根据透明，可审计和效率原则进行保管和经营。平台盈利分别被多重签名钱包保管，并受公众的审阅。对于安全问题，这些多重签名钱包的私钥是由五位值得信赖的个人控制。钱包执行任何付款，都需要这五个人的同时签名。平台收到的资金将不会用于GMC开发方的股东分红或利润分配。而会全部用于GMC的开发、维护等技术工作以及GMC的生态系统建设（例如投资培育GMC上的各类应用等）。

风险披露

在GMC的开发、维护和运营过程中存在着风险，这其中很多都超出了开发方的控制。除本白皮书所述的其他内容外，GMC的每一参与者还均应细读、理解并仔细考虑下述风险，之后才决定是否参与本平台项目。

参加本平台项目应当是一个深思熟虑后决策的行动，将视为参与者已充分知晓并同意接受了下述风险：

1、因法律政策变化或政府行动，导致GMC无法正常开发或使用，或者导致GMC币被禁止持有或使用的风险；

2、因密码学的发展或者量子计算机的商用化，导致基于密码学的货币不再具有足够安全性（比如私钥易被破解）的风险；

3、因GMC的技术开发难度较高，因此导致的开发失败的风险；

4、因本平台项目所获得的ETH或BTC失窃，导致GMC开发缺乏资金支持难以为继的风险；

5、GMC的源代码存在瑕疵、缺陷和漏洞所导致的GMC运作过程中各种故障问题的风险；

6、GMC的源代码基于社区要求而进行升级或修改，因此导致无法预测的风险；

7、GMC在运转时被“分布式拒绝服务”攻击或其他类型的攻击的风险；

8、任何人持有的GMC币被盗窃、遗忘或灭失的风险；

9、GMC币缺乏二级交易市场、价格不稳定或没有其他人愿意购买GMC币的风险；

10、与GMC具有同类功能或存在竞争关系的其他区块链的开发、运营，以至于GMC 被边缘化或排挤出市场的风险；

11、由第三方开发的GMC上的各类应用存在的故障和缺陷所引发的风险。