GFCC 公链白皮书

V1.0

目 录

一、概述

1.1 项目背景

区块链是一种在对等网络环境下，通过透明和可信规则，（按照时间戳顺序）构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务（交易）处理的模式。是一种分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，具有分布式对等、数据块链式、不可伪造和防篡改、透明可信、高可靠性等关键特征。

如今，随着各种区块链项目的兴起与发展，人们不断见证着区块链技术为各个领域带来的变化，也逐步提升区块链技术本身所呈现出的价值，如数字资产的确权、无需第三方机构建立的信任体系、自动化的智能合约、价值共享等。

区块链生态构成主要包括区块链网络、基础设施（如资产管理、记账节点、交易模型等）以及运行在区块链网络上的智能合约。自 2009 年比特币网络成功运行以来，区块链各类技术得到了突飞猛进的发展，尤其是底层技术。区块链平台根据去中心化程度、应用场景的不同，可划分为三类：公有链、联盟链、私有链，不同的区块链平台在准入机制、共识算法等诸多方面存在着一些差异。

三种区块链部署模型：

1、公有链：任意客户都可以使用，任意节点都可以进入，所有节点共同参与共识和读写数据，较强的去中心化特征，案例：比特币和以太坊；

2、联盟链：只有利益相关的客户才能使用，节点只有授权许可才能接入，接入节点按规则参与共识和读写数据，较弱的去中心化特征，案例：Hyperledger Fabric；

3、私有链：单个客户使用，仅有授权的节点才能接入，并按照规则参与共识和读写数据。

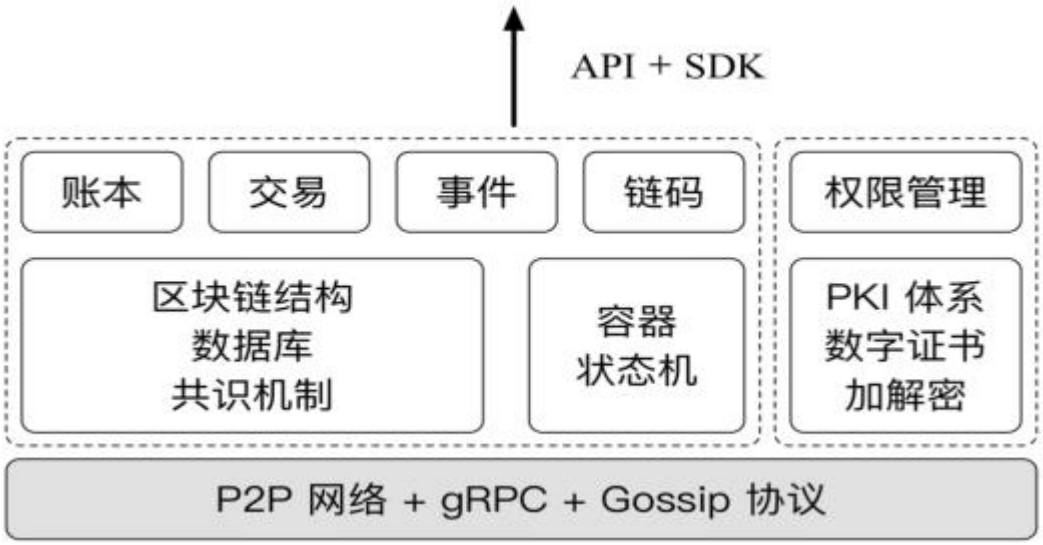
总体来说，目前区块链技术仍处于初步探索时期，绝大多数平台在设计上都未成熟，没有充

分体现出区块链技术的独特优势。GFCC 公链基于现有的区块链底层技术基础上，首次提出先出块后验证的理念以及改进的 POS+POW 混合共识机制，在安全性、性能、高可用性等方面实现较好的平衡。

二、系统架构

2.1 基础业务架构

在系统设计上，GFCC 公链采用分层设计，系统采用前端应用层、中间接入层、区块链层、数据层，各层之间独立部署，通过异步协议交互，如下图：



GFCC 公链是一个支持主链和侧链的区块链网络。有一条特殊的链，叫 Root 链，Root 链管理网络中的其他平行链，并提供跨链服务。其中 Root 链提供如下独立功能：

A 创建独立的侧链。

B 提供与各个侧链的数据交换协议，支持侧链间的数据交换。

C 提供基础共识机制与安全管理机制，管理整个网络的正常运行。

2.2 账户余额模型 vs UTXO 模型

现阶段，整个区块链网络的记录存储模式可以分为两大类：以以太坊为首的账户余额模型和以比特币比特币为首的 UTXO 模型。

UTXO 模型是通过链式的方式组织所有交易的输入和输出，每一笔交易的输出最终都能追寻到一个币基交易，在比特币中也即被挖出区块的奖励交易。由于在 UTXO 中没有账户的概念，所以并行地处理交易不会出现任何问题，同时不可变的账本能够让我们在节点快速更新时，也能分析某一时刻整个网络中数据的快照。

在 UTXO 模型中，当我们需要计算某个地址中的余额的时候，需要遍历整个网络中的全部相关区块，同时，并行处理交易虽然可行，不过并行地创建交易却会出现很多问题，例如多笔交易使用了同一个 UTXO，会导致双花，最终只有一笔交易会被网络接收。

相比于 UTXO 模型，账户余额模型更加容易理解，账户余额模型其实就是一个巨大的状态机，其中的状态都是由多个账户组成的，交易仅仅体现的是账户余额的变化。

我们认为 UTXO 相对于账户余额模型，并发性能更好；但是在扩展性以及使用便捷性上，账户余额模型表现得更好。

由于在 GFCC 公链中，我们引入了先出块后验证交易的理念，出于对性能和扩展性、便捷性等的综合考虑，我们采用账户余额模型来实现账本的存储。

GFCC 公链在账户余额模型的基础上做了智能合约的扩展，提出链外合约的概念，在扩展区可加载各种不同的合约虚拟机，每个合约虚拟机都需要实现运行合约和回滚合约两个接口。回滚机制是为了应对先出块后验证机制而设计的，也即在验证交易时一旦发现问题，合约状态可实现回滚。我们在合约回滚方面进行了几个方面的优化，合约开发者可以根据具体应用场景选择合适的实现方式：

A 由开发者自行实现回滚逻辑。

B 利用区块链数据操作日志，自动生成回滚逻辑。

三、信任的交易模型

3.1 基于区块链的信用交易评价体系（历史交易数据）

现有的信用评价体系都是基于历史的交易行为进行分析获得，如果没有历史交易行为，就无法建立准确的信用评价体系，而这些历史交易行为数据往往都是由某个机构独立占有，而参与信用评价体系的机构的违约风险是比较高的。

区块链技术在提升数据的真实性和安全性方面的作用在建立信用评价体系方面表现出更为明显的优势。比如某些违约记录、违规记录等数据是非常适合进行链上存储的。而在数据链下存储的场景中，区块链设置的校验机制可以保证数据的真实性。在一个良性的校验机制下，数据之间的校验结果出现差异时，区块链系统可以根据机制自动判断并返回结果。同时，区块链系统的校验机制奖励提供正确信息的人，激励参与者继续提供正确的数据，另外区块链系统惩罚提供虚假报告的人，甚至可以将虚假数据提供者的信用水平下调。未来虚假数据提供者再次提供信息时，可信度将会降低，对信息结果的影响程度下降，从而提供整个系统的数据的可信度。

在基础安全机制特别隐私体系有保障的情况下，通过区块链的投票机制及奖惩机制的设计，可以期望用户贡献更多的、更为准确的数据。基于区块链的信用评价体系，用户既不用担心提供真实的评价会泄漏自己的隐私，还会因为提供真实的评价而得到奖励。

区块链技术的去中心化和自治性的特点，对于交易行为的信用评价体系的建立起着至关重要

的作用。

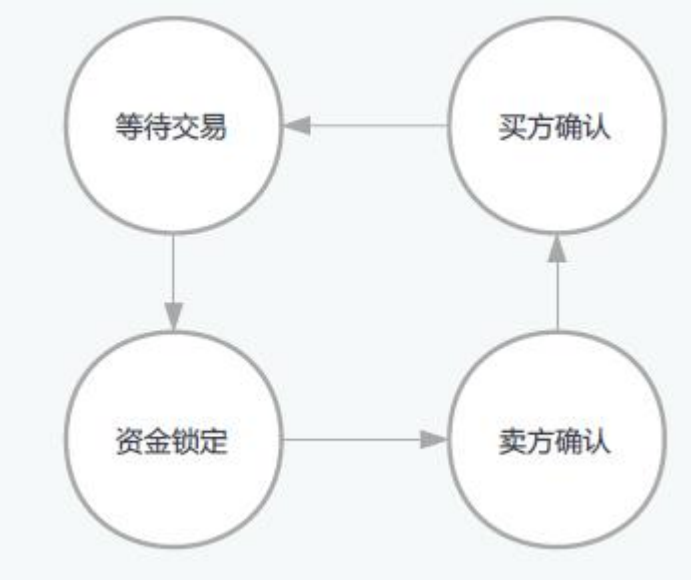
去中心化是指在基于区块链的网络结构中每个节点都共享网络中的所有数据，网络中不存在一个中心节点或者核心节点，每个节点都是平等和自由的，也即体系中每个成员既是自己行为数据的来源又是整个系统的管理者和维护者。同时数据的各个组织间通过共识机制保证整个网络的透明性。

自治性是指节点或成员都是自由接入或自由退出区块链网络的，而且任何节点在接入区块链网络后，会自主地监听其他节点或账户发生的数据信息的修改并随时进行验证，整个流程都是区块链网络自主实现的，不需要人工进行干预，没有节点拥有绝对优先的权利。

在过去的若干年内，区块链技术和社区一直在致力于开拓基础协议和基础架构层的关键性技术，如今，区块链这一革命性的技术可将信用评价体系提升到一个更高的层面。基于区块链技术的安全的信用数据交换网络可以提升数据质量、降低数据采集成本、扩大数据覆盖范围，并最终通过大数据打造更好的信用评价模型。

3.2 抵押冻结担保交易模式

GFCC 公链通过在链上实现担保交易协议，为交易行为提供了去中心化的第三方保证服务，最大程度地保证“一手交钱，一手交货”的交易过程，保护买卖双方的利益。



担保交易的简单执行过程如下：

(1) 卖方在区块链上挂单，输入售卖资产的信息，包括资源 ID、特征值、卖方帐号、金额等参数，等待需求方发起交易。

(2) 资产需求方在链上合约中转入指定的金额，合约检查转入金额是否满足售卖要求：若检查通过，则记录该事件，资产进入资金锁定状态；若检查未通过，则向转入者反馈错误信息，进入等待交易状态。

(3) 卖方提供数据后，向合约发起确认，并设置有效期。若有限期结束时仍未执行其他操作，则合约自动进入结算过程。

(4) 买方收取资产完成后，向合约进行确认。

(5) 合约将资金转到卖方账户，过程结束。

以下通过一个具体的案例来描述 Alice 售卖 a 个单位的资产给 Bob 的解决方案：

首先 Alice 创建一个随机的字符串 x，计算哈希值 h=H(x)，Alice 创建一笔可以退还资产的交易 A，但并不公开，Alice 将交易 A 发送给 Bob，让 Bob 签名。一旦 Bob 对交易 A 签名，Alice 公开交易 A。

Bob 创建可以退还数字货币的交易 B，但并不公开，Bob 将交易 B 发送给 Alice，让 Alice

签名，一旦 Alice 签名，Bob 公开交易 B。

情景 1：Alice 按照计划完成兑换，把 x 给 Bob，流程结束。

情景 2：Alice 改变主意，想要终止交易，Alice 只要不向 Bob 公开 x 的值即可。

四、GFCC 公链的解决方案

4.1 GFCC 公链技术原理

GFCC 公链技术从开始就选择的是授权的联合区块链技术，从逻辑角度理解，相对于全面开放式共识的区块链没有那么彻底的开放，GFCC 公链会带有一定来自核心的管理规则和认证，避免了公有区块链的完全自治而导致的不可控风险。同时，GFCC 公链技术源于其在近三年时间建立的虚拟社区网络所组织建构的社会化网络结构而实现的有组织的去中心化管理机制，这种机制与区块链技术结合，形成基于人类社会的去中心化+基于区块链的货币的去中心化，这两个去中心化的同步实施，形成两大特征，缺其一都会成为去中心化进程的不完整状态，必然难以为继。因为这个社会是人的社会，不仅仅是货币．当然科技、文化、商业等进程依然需要货币的参与，所以社会化网络和区块链技术的结合，两个去中心化的结合，相辅相成才是区块涟技术的未来，才是社会化网络的未来。

GFCC 公链其本质是一个结合去中心的社会化网络的公有区块链系统，相对于目前常见的公有区块琏模型所应用的仅仅是发行电子货币，而无实质性结合社会、结合人的社会行为的应用。

可以简单的说，GFCC 公链系统已经将人和人的社会与区块链技术相结合。而目常见的公有

区块链（比特币、以太坊）还仅仅是一个理论和实验产物，而目区块链技术的方向也是需要落地到社会中，形成一个去中心化的社会形态，是一个去中心的人的互联、社会的互联，这一点，GFCC 公链系统已经落地目具备可操作雏形。

GFCC 公链不同于传统区块涟在保留了区块琏技术的必备特征以及安全持点的前提下，结合社会化网络的复杂需求，形成了适合于实现自组织机构、分布式节点互信社交网络及蕴含的相应经济社会制度的社会化区块链系统，把个体的人和商品、贸易和货币、组织和社会全部通区块涟融合在一起。

4.2 GFCC 公链的去中心化分布式存储系统

为解决目前区块链技术的区块仅能记录交易数据而不能记录文件内容，所以 GFCC 公链基于 IPFS 技术开发了一套智能合约应用，GFCC 公链系统能够弥补现有区块链系统在文件存储方面的短板：区块链只能记录交易数据，而不能支持大文件存储的缺点，GFCC 公链系统将文件永久存赭和区块链的特性高度结合，将被广泛应用于保护版权、身份证明、来源证明等。

GFCC 公链系统作为全球区块链的基础设施，会随着区块链技术的发展而发展，成为全球去中心化文件存储的核心，并为未来区块快速发展提供充足动力。共同构建去中心化的网络世界。

分布式记账需要全网记账节点的参与，在通常的公有链模型下通矿工的竞争获得记账的权力，并获得相应的 token 的奖励，这些竞争的方式都会带来效率低和资源的严重消耗，

导致记账成本高昂，也是目前区块链普遍存在的问题，因此，GFCC 公链分布式存储设计了一套创新的全网记账的逻辑，能够提升记账效率的同时不会产生无效的资源浪费，通过 GFCC 公链分布式存储系统使得节点在完成存储业务的同时进行 GFCC 公链的记账工作，但并不是每个节点都有记账权利的仅授权节点具备记账权。

GFCC 公链系统能够支撑未来全业务区块链生态的发展，通过开源的生态形成多样的智能合约应用而服务于用户。同时，基于 GFCC 公链系统也能够对于提供文件存储服务的节点给予相应的奖励和激励，从而扩大 GFCC 公链系统的服务能力。

4.3 GFCC 公链核心组成的区块链投票系统

Gvote 是基于 GFCC 公链的智能合约应用，但又是 GFCC 公链的核心基础。Gvote 不仅提供群体智能服务，最重要的是提供了 GFCC 公链未来发展的所有的全体决策，GFCC 公链通过 Gvote 成为真正意义上去中心化区块琏系统。

1．创世：创世是指 GFCC 公链社会化网络发展的初期由公司行为来辅佑其初期稳定发展的代称，随着社会化网络去中心化的发展最终形成一个概念而无权力。

2．成员：社会化网络的成员，每个会员都是现实社会中的真实个体，通过一定规则相组合形成社会化层级概念，形成虚拟的立体结构。商业行为、市场行为、社交行为等都以这个分支为唯一分支，这个分支是正常的全社会形态的网络化

3．记账者：被 GFCC 公链授权记账节点的所有者，其也是 GFCC 公链的成员但又高于成员身份，同时具有相对于成员更高的建议权和参与权。相对于成员员来说其有更好的在不同行业、学科的能力和学术理论，这个分支代表着社会化网络发展中的决策建议功能。

通过 GFCC 公链的投票权系统（Gvote）实现投票过程中的身份验证、匿名投票、隐私保护、票权计算等稳定与有效，实现区块链技术为基础的票权系统，参与 GFCC 公链规则及未来发展方向的建议和意见，能够强力促进社会事物的大众方向。是社会化网络去中心化进程的基础。

基于上述 GFCC 公链技术的社会化特点：将社会的人和区块链技术紧密结合。

这三种社会结构分支，代表三种力量，相互制衡、相互发展，以去中心化为发展方向。通过健全、高效、安全的票权系统（以区块链技术为基咄）形成最终的去中心化组织结构。

4.4 算力挖矿与抵押收益的平衡

在 GFCC 公链中，有两种矿工节点类型：基于 DPOS 的出块的节点、基于 POC 验证区块数据的节点。这两种矿工节点都是需要产生收益的。

这两种矿工节点的收益如何有效地分配是我们需要解决的核心问题之一，如果 POC 矿工的收益高于 DPOS 矿工的收益，则 DPOS 矿工没有足够的动力产生区块；反过来，只有最底层的 DPOS 矿工的收益高于 POC 矿工，POC 矿工就需要积累足够的信用值升级为 DPOS 矿工。底层的 DPOS 矿工为了获得更高的收益，需要努力提升自己的诚信度、对网络的贡献，只有这样底层的 DPOS 矿工可以升级为更高层权限的矿工。

在传统的基于 POC 的挖矿设计里，51%的算力攻击是指掌握了全网 51%的算力之后，用这些算力来重新计算已经确认过的区块，使区块链产生分叉从而使得自己获利。而在我们的系统里，POC 矿工只有执行验证和提交验证结果的权限，在理论上，POC 矿工获取收益的唯一方式就是做诚实的矿工。

作为 DPOS 矿工在出块阶段如果选择不诚实的记账，在 POC 验证阶段会被发现并在最终被系统恢复，DPOS 矿工的任何不诚实行为都会导致该矿工会被除名，而且作为 DPOS 矿工在担任出块节点时，是需要抵押一部分收益的，这一部分收益也会被 POC 验证节点收回。所以无论如何，DPOS 矿工在出块时选择作弊是没有收益的。

在经济学的理性人的假设前提下，无论是 DPOS 矿工还是 POC 矿工都是追求自身利益的最大化，只有 DPOS 的挖矿收益高于 POC 的挖矿收益，POC 矿工才有动力提升自己的诚信度和贡献，从而有机会转化成 DPOS 矿工。另外 POC 矿工在验证阶段除了挖矿本身的收益外，还可额外获得发现作弊的 DPOS 矿工的抵押收益，这就给 POC 矿工一种理性选择：尽可能多地发现不合法的区块和交易。

另外需要注意的是，在我们的 DPOS 矿工的设计中，权益不仅仅是其他权益系统中设计的单纯以币龄作为权益，而是在权益的计算中引入了信用值。DPOS 矿工不仅仅需要保证足够的币龄，还需要不断提升自己的诚信度才有可能获得更大的收益。

五、技术细节

5.1 侧链的架构

侧链的概念最早是由比特币社区提出，而后侧链技术更多是在关注和描述比特币相关的扩容，它的定义是：可以让比特币安全地从比特币主链转移到其他区块链，又可以从其他区块链安全地返回比特币主链的一种协议。

比特币的闪电网络也可以认为是一种侧链技术，因为它允许用户 A 和用户 B 不在主链上直接进行交易，而是在“侧链”上进行频繁地进行 N 笔交易之后，再把最后的交易结果同步到主链上。

侧链的本质是，首先把你的一部分比特币币（或以太币）锁定在主链上，并且在侧链上对你

的数字货币进行操作，当操作周期结束之后再在主链上进行结算。

在 GFCC 公链中，我们希望打造一个环境来让可互操作的竞争性易于创建和使用，但不会产生不必要的碎片，需要满足如下特性：

A 在侧链间转移的资产应当能够被当前持有者移回，但除此之外的任何人都不行（包括之前的持有者）。

B 资产的移动应当无交易对手风险，也就是说，不诚实的一方无法阻止转移的发生。

C 资产转移应当是元操作，也即原子操作，也即，要么完全完成，要么根本没有发生。不应存在会导致资产损失或允许欺诈产生。

D 某条侧链发生发生资产被盗或缺陷行为的时候，不应该导致其他任何侧链或主链发生资产丢失或被盗。

E 区块链重组时应该处理干净，即使在资产转移期间也要如此。任何破坏也只能发生在它所处的侧链上。理想情况下，侧链应该完全独立，其他链上的全部所需数据由用户提供。侧链的验证者应当只有在侧链本身的显式共识规则有要求时，才需要跟踪其他链。

早期转移数字货币的解决方案是用一个可公开识别的方式来销毁比特币，让新的区块链能检测到，以允许发行新币。这解决了上面提到的部分问题，但由于这种方式只允许单向转移资产，还无法满足目的。

我们提出的方案是由资产转移的交易本身提供所有者证明来转移资产，避免让节点有跟踪发送方链的需求。当资产从一个侧链向另一个侧链转移时，我们在第一个侧链上创建交易并锁定资产，然后在第二个侧链上创建一笔交易，该交易的输入中包含一个锁定已正确完成密码学证明，这些输入用某种资产类型来标记。

其中第一个区块链，我们称之为父链，第二个则称为侧链。在我们的侧链设计中，资产从初始父链转移到一条侧链上时，可能还会再转移到其他别的侧链，最终还是能再转回至父链，

并保全初始资产。

此外，由于侧链是从父链中转移现有资产而不是另外凭空铸造新的资产，侧链不会引起未经授权的铸币，维护资产的安全和稀缺性依靠父链来实现。

由于侧链还是一个独立于主链系统的区块链，它们可以自由地尝试新的交易设计、信任模型、经济模型、资产发行语义或者新的加密特性，这些给我们未来探讨一些新的侧链模型的可能性。

最后有必要提一下基于侧链的资产发行机制，大多数情况下，我们认为侧链不需要自己的原生数字货币，所有侧链上的币最初都被锁定，直到来自其他某条侧链的资产转入将其激活。不过，侧链也可以制造自己的代币，或者带有自己语义的资产发行。它们可以被转移给其他侧链来换取其他的资产和数字货币，整个过程不需要对中心方有信任，即使将来赎回时对可信方有需求。资产发行有很多应用场景，包括传统的金融工具，如股票、债券、凭证或白条等，这使得外部协议可以将所有权及转账记录跟踪等授权给发行所有者股份的那条侧链。发行资产链还可支持更多的创新工具，如智能财产。

5.2 数据隐私保护与监管的平衡

近期，关于区块链内隐私保护的新特性引发很多的讨论，在逻辑上，数据的隐私保护和数据的可监管性是一对矛盾的关系。在 GFCC 公链中，我们设计的一个重要特性就是多通道的支持，使用多通道的特性，账本网络中若干成员可以协商构建一个专属通道与外部隔离，通道外部的节点无法看到其中的账本和交易数据，极大的提供隐私性。对于超级监管权限的账户，通道需要提供一个可供查看的权限入口。

然而，在有些场景下，单纯使用通道来保护数据安全仍然存在不足：

A 虽然外部节点无法看到通道内交易数据，但验证服务可以看到所有通道的所有数据。

B 通道内的节点能看到通道内的所有数据，即使跟自己无关的交易，也就是说，粒度还是比较粗。

C 为了保护任意多方之间的隐私，需要构建大量（O(n^2）数量级)的通道，而通道是比较重的资源。

D 某些时候，成员对数据的访问控制需要一定的动态性，通道机制无法完全满足。

总之，需要一些更灵活的方案，来实现更细粒度的数据隐私保护。

首先，我们在以下环节进一步改进隐私性：

A 记账过程：客户端将交易提案发送给相关记账节点后，记账节点利用链码进行模拟执行，对结果的读写集合进行签名，返回给客户端。在这个过程中，客户端可以选择将需要保护的私有提案只发送给选中的若干节点（授权组）进行背书。但节点可能会动态加入或退出授权组，并且客户端无法保证实时获知授权组的变化，因此授权组内的节点之间要能相互传播私有数据。

B 排序过程：客户端根据背书结果构造合理的交易请求（带有读写集），发送给排序服务，排序服务对交易进行排序和打包出块。在这个过程中，排序节点显然不需要访问交易内容。为了增强隐私性，客户端不能将私有交易的内容直接发送给排序服务。

C 验证过程：在这一环节中，完成交易提交的节点必须能获知交易的读写明文。为了避免所有节点看到明文，需要本地建立隔离的状态数据库和链结构来专门存放私有交易数据。

需要说明的是，当授权组需要支持动态增加和删除时，则需要非常复杂的机制。在 GFCC 公链的初始版本中，我们会选择静态授权组的方式，通过对链码进行实例化的时候进行静态指定。

六、多元身份体系认证网络

6.1 个体身份认证

在 GFCC 公链中，任何涉及到用户主体或节点主体的相关数据访问、交易、生成区块、验证交易等都需要得到所有者的授权。为此，我们设计了一套用户授权协议来保护用户的数据安全和数据隐私。协议利用可验证的技术完成异步验证授权，同时支持托管授权和细粒度访问控制的授权策略。

首先，在涉及到用户授权的协议中主要涉及到的角色有：

A 普通用户：对资产拥有所有权的实体，能访问自己的数字资产以及数字凭证，能自由发起转账交易、查询账务情况的用户。

B 区块链账本生产者：主要是被授权记账的节点账户，他们在系统中类似于联盟链的记账模型，由所有用户参与投票或由系统委托受信任的节点构成。在系统运行过程中，根据节点的行为质量动态考核，通过去中心化的自组织方式运行。

C 区块数据验证者：对于生产者产生的区块，验证者负责对区块的交易的有效性以及权限等等进行验证。

D 区块数据修改者：区块数据的修改者身份由生产者担任，根据前面介绍的算法进行选择合适的区块数据修改者。

在 GFCC 公链中，个体（基于以上任意角色的一种）接入网络仍然是采用数字身份认证的机制。早在 1984 年，Shamir 提出了基于身份的密码系统，在一定程度上解决了用户身份与公钥的绑定问题，在 2006 年，Paterson 和 Schuldt 构造了标准模型下可证明安全的基于身份的数字签名方案，但由于计算效率不高，很难在实际应用中使用。可信数字时间戳服务可以为电子文件提供日期和时间信息的安全保护，但无法保证电子文件本身签名的合法性。。手写签名识别技术经过多年的研究已经相对比较成熟，尤其是在线手写签名识别，通

过电子手写签名设备来采集书写过程的动态信息，可以有效标识签名者的身份，但仍然无法完全替代纸质签名。

在这里，我们采用基于数字签名的统一身份认证体系。在一个实际的安全接入平台整体架构中实现的身份认证系统主要包含终端信息收集、数字证书的 USB-Key 以及统一身份认证系统这三大功能模块。考虑到平台的交互性，区块生产者和区块数据修改者在接入身份认证过程中采用传统联盟链的结构，通过发放数字证书并接入第三方具有权威公信力的认证服务器做数字身份认证。

对于普通用户和区块数据验证者则采用类似于比特币、以太币等公开的离线的帐号生成体系，账户只要满足程序要求的格式，均可自由接入和退出。

这里特别强调的是，对于区块生产者的认证过程采用双向注册的机制。双向注册是指授权服务向资源提供方注册自己的地址，以便资源提供方在处理资源访问请求时，给资源需求方返回授权服务的地址。同时，资源提供方也需要向授权服务注册自己的地址，以便用户对数据进行访问控制。

以下是一个典型的双向注册流程

另外利用基于属性的访问控制，所有者能够设定灵活的访问控制策略，限制特定的资源能够满足由特定属性条件的请求者访问。

授权服务接收到授权请求后，通知用户进行授权操作。对于满足授权条件的资源访问者，用户为其签发授权证明。在授权证明的有效期内，资源需求方可以重复访问数据而无需再次申请授权。

6.2 多元身份密钥的融合管理

GFCC 公链不仅提供基于纯粹数字签名的身份认证体系，还提供多元身份认证融合的管理系统。多元身份认证不同于以往的单一身份认证体系，多元身份认证可以为实体提供融合了外部身份信任源认证以及实体间背书的多元认证体系，不但可以为实体提供“我是谁”的基础身份认证，还可以进一步为实体提供诸如我拥有什么、我喜欢什么、我经历过什么等多维度数据的身份信息，进而形成多元的认证体系。

多元认证协议包括以下两种模式：

A 外部信任源认证：GFCC 公链以自签可验证声明的形式给 ID 绑定外部信任源，任何实体都可以通过验证 ID 绑定的外部信任源来验证实体的身份。实体身份认证的可信任程度由 ID 绑定的外部信任源的公信力和认可度来决定。

B GFCC 公链实体间的身份认证：内部的实体还可以通过内部的其他实体签发声明的方式实现身份认证。

外部信任源认证支持自我导入和信任锚导入两种方式。

A 自我导入：用户通过社交媒体、银行 UKEY 签发等方法来绑定现实信任，该模式利用了现实世界已有的信任（比如微信、Facebook、银行等）。原理实际上很简单，首先用户在 GFCC 公链上添加一个外部信任源的证明地址，用户接着在该证明地址上提供一个可验证的声明，保护如下内容：声明创建日期与过期日期；声明的内容包含声明的类型、ID、社交媒体类型、社交媒体的用户名等；需要指定使用者的公钥，必须是 GFCC 公链中包含的公

钥列表中的一个。

当第三方需要验证用户的外部身份时，首先在 GFCC 网络中读取到用户信任源的证明地址，然后到这个地址去获取可验证的声明，最后验证该可验证声明即可。正常情况下，用户的社交媒体账户基本只能由其本人方可进行管理，也就是说只有其本人才能够发表一个可验证的声明。

B 信任锚导入：信任锚通常是指那些经过了实名认证，且在社会中由一定公信力或声望的政府单位、非营利组织以及社会名人等。成为信任锚需要遵守 GFCC 公链的一系列标准。信任锚使用自有的认证方式对被认证实体进行认证后，对被认证实体签发一个可验证的声明。声明中不需要包含被认证实体的真实身份信息，仅记录实体及认证服务的 ID，作为该服务的认证结果即可。

正是由于可验证声明的开放性，使得 GFCC 公链中任何实体可以对任何另一个实体就任何事情发表声明，这也使得网络中的身份认证远远超过传统的身份认证概念。这种多角度、多方面的认证相比传统的单一认证更准确、更全面。

6.3 不同信任场景的私钥授权体系

不同的信用场景管理是每个区块链系统都需要面对的问题。对于传统的公链项目，比如比特币的信用场景管理是非常粗放型的，对于大量的小额交易和大额交易，使用的是同一种管理机制和信任级别。

对于大量的小额交易来说，是否真实需要这么高的可信性呢？闪电网络通过在交易双方之间建立一个“微支付通道”来解决大量小额支付的问题，双方都预存一部分资金到“微支付通道”里，之后每次交易，就对交易后的资金分配方案共同进行确认，同时签名作废旧的版本。当需要提现时，将最终交易结果写到区块链网络中，被最终确认，可以看到，只有在提现的

时候才需要通过区块链。

借鉴于闪电网络的思路，GFCC 公链拟在闪电网络基础上构建更细粒度的信用场景管理，每次交易发起的时候，根据交易的参数匹配对应的信任级别，不同的信任级别对应的网络消耗不同，相应消耗的手续费也是不同的。

不同于闪电网络，由于在 GFCC 公链中，账本是采用分层模型实现的，不同的层级的记账者掌握着不同的资源权限，记账者的级别越高，其享有的权限和信任级别越高。这样，我们就可以将不同的交易类型和参数量化成不同粒度的信任级别，并匹配不同的共识级别。

比如对于小微支付而且重要性不高的交易类型，只需要最底层所在的域的记账节点进行记账即可，对于稍重要的交易类型，可能需要上一层级的域对应的记账节点进行记账；对于重大系统级的交易类型，则可能需要顶级节点参与记账。

当然，对于不同级别的记账节点在申请加入网络过程中都是需要严格地授权的。而不同层级的记账节点的授权都是直接依赖于上一层节点。

6.4 见证人（代理人）的管理体系

在 GFCC 公链中，见证人负责收集网络运行时广播的各种交易并打包到区块中，其工作类似于比特币网络中的矿工，在采用 POC 容量证明的网络中，是由一种获奖概率取决于哈希算力的抽奖方式来决定哪个矿工节点产生下一个区块。而在采用 DPOS 机制的网络中，一般会采用投票机制决定见证人人选。

GFCC 公链跟其他基于 DPOS 共识的区块链系统类似，也是需要通过见证人机制来防止作弊。在系统中，见证人是没有限制的，任何用户都可以提交申请参与竞选，在缴纳相应的保证金后就可以成为候选见证人，最后通过选举产生最终的见证人。

见证人是提前被系统随机分配并公布，一段时间后会重新选举并分配新的见证人，所有见证

人会共同分享被见证用户支付的交易费用。

跟传统 DPOS 机制的见证人机制不同的是，我们的见证人是可以竞选更高级别的见证人，见证人级别在上升过程中必须保证自己的信用等级是足够的，一般见证人出于利益的考虑，为了获得在竞争中的优势，诚实担任见证人是制度约束的结果。

6.5 仲裁者的管理体系

跟其他区块链系统一样，GFCC 公链依然存在着纠纷的可能，在我们的设计中，仲裁系统又可以叫做争议解决层，也是中间层偏行业的重要组成部分。随着 dapp 和侧链资产的发布，就像互联网上网购的一些小纠纷类似。在生活中如果出现了纠纷，我们会走法律程序，在 GFCC 公链中，我们通过去中心化的办法解决争议。

由于在区块链的世界中，钱包和身份是一一对应的，因此在出现纠纷的时候，争议双方可以分别将他们钱包里的信息作为证据提交到链上。然后，仲裁系统会随机抽取“陪审团”盲审。由于陪审团是由系统随机抽取的，陪审团并不知道具体是谁，也不能事先贿赂。陪审团成员只能看到事件本身，然后从事件的信息作出判断后进行投票，确定事情的结果。

另外在陪审团盲审阶段，陪审团还可以讨论问题、提出疑问，整个系统是去中心化运行，每个人都是匿名的。匿名性也决定了陪审团不会有主观倾向，而这一点是传统手段很难做到的的事情。

在我们的区块链系统中，仲裁协议是通过一个仲裁的基础智能合约来实现，因为智能合约是在虚拟环境中执行，是一个封闭的环境，合约无法与外界直接通信或取得任何数据。而 Oracle 语言机可以为区块链智能合约提供可信的链外数据，用来触发智能合约顺利执行的数据来源。其中 Oracle 可以通过监听特定的事件来接受合约所发出的请求，处理完成之后再由 Oracle 主动调用合约的回调方法将数据传回。所以仲裁服务将使用 Oracle 完成区块

链和平台之间的一系列服务。

仲裁合约为了确保信息的可靠安全，数据提供了基于 TLSNotary 的可信证明技术。TLSNotary 证明主要基于安全传输层协议 TLS1.1，TLS 用于在两个通信应用之间提供保密性和数据完整性，其最大的优势就在于独立于应用协议，更高层协议可以透明地分布于 TLS 协议上面。

另外仲裁协议提供了一个案件信息账本，用于保存所有案件的相关信息，比如合约的内容、投票结果、投票原因、参与的陪审团成员、仲裁结果等等。然后在主链上会存储案件数据的哈希值，以确保证据数据的安全性和不可篡改性。

陪审团的节点负责监听部署在公链上的 Oracle 所发出的事件请求，所有的节点都将共同监听，收到事件信息后会和附近的节点进行对比和确认，一旦超过半数以上确认无误之后会开始运行节点随机筛选算法，用当前的时间戳加上最新的区块的索引和 Oracle 提供可信的随机数。然后每个节点会算出一个节点的编号，获得更多选择的节点将被选为当前的记账节点，负责将当前案件的信息记录到仲裁账本中。

在应用层，仲裁合约会提供案件展示、案件创建、证据上传、参与投票等功能，以方便用户更便捷地处理案件和保持对案件的持续关注。

七，智能合约

长期以来，人们一直在致力于通过法律、技术等方法来建立信任机制和解决信任问题。经验表明，传统的解决方案很难建立一个系统化和标准化的信任机制来应对各种各样的日常业务需求，随着互联网技术的发展特别是区块链技术的广泛应用，基于公钥密码学、去中心化、可溯源、不可篡改的公共账本等机制在技术上实现了信任。早期的区块链技术如比特币等只

是实现了一种去中心化的发行货币和记账的方式，是以太坊这种被冠以区块链 2.0 的技术真正把区块链的信任机制通过一个叫做“智能合约”的工具带到了人们的眼前。

其实智能合约最早是由密码学家 Nick Szabo 在 1994 年首次提出，他当时给出的定义如下：一个智能合约就是一套以数字形式定义的承诺，其中包括合约的参与方可以在上面执行承诺的协议。

在 Szabo 提出智能合约的近二十年的时间里，一直都没有如何将智能合约的理论用到实践中的清晰思路，直到区块链技术的出现及发展，给智能合约带来了可信任的执行环境。事实表明，以太坊的智能合约的设计是非常成功的，目前已经有数以千计的智能合约正运行在以太坊的网络上。

然而就在智能合约在区块链的世界炒作的同时，我们也注意到很多失败的智能合约项目，这并不是说人们缺乏利用智能合约的想法，而是很多想法根本就无法在现有的智能合约架构体系中实现，观察目前的智能合约应用代码，我们会发现基本的逻辑都是限定在发行代币、公平投票、轻量级的融资、资产拍卖等，而且这些逻辑行为还强耦合于代币的交易行为。究其根本原因，我们会发现现在的智能合约架构其实是被存储在区块链上的一段代码，由区块链上的代币交易行为触发代码的执行，它能读取并在区块链的数据库中写入数据。虽然智能合约的代码被设计成图灵完备的语言来实现，但是代码的行为又受到具体交易行为的限制，具体来讲就是内部代码执行的行为所依赖的外部数据仅仅是该代码执行时被触发的具体交易数据，这就将智能合约的代码行为限制在区块链的交易行为生态内部。另外由于区块链是基于共识的系统，这意味着只有在所有诚实的矿工节点在执行相同代码后所有节点都必须要达到相同的状态，合约的数据才会起作用，如果无法做到这一点，整个系统将变得毫无价值，这也进一步限制了智能合约的应用范围。从合约的执行过程来看，每次合约的代码是由交易触发然后由矿工节点参与执行，本质上相当于我们是与矿工节点在签订合约，这就相当于代

码执行权限、数据存储权限、数据验证权限都在矿工节点手上，就意味着合约本身的信任价值严重依赖于底层区块链技术。

另外我们也会听到很多关于智能合约应用的一个较为经典的例子，使用智能合约来自动化完成支付行为，这个想法的意思就是在某个条件达成的某个适当的时机，智能合约会自动启动支付行为，这样既避免了手动支付同时又能保证支付行为无法违约。然而在现有的智能合约架构中，这个过程是根本无法通过系统内部自治完成的。

目前智能合约在设计中一直在过多强调扩展性，比如 solidity 编程语言被设计成图灵完备的编程语言也是基于扩展性的考虑，但是扩展性强的同时也带来了一些安全的隐患，比如著名的 The DAO 攻击。Solidity 语言是为以太坊平台开发的，该语言未经过测试，最为重要的是目前还没有一套完整的针对智能合约的形式化验证工具。而且当前智能合约与以太坊的区块链耦合度比较高，一旦区块链发生问题，智能合约所涉及的交易信息也会受到牵连，另外如果智能合约出现安全漏洞，意味着区块链上的交易数据也会受到影响。研究表明，以太坊的 Parity 钱包漏洞使得用户财产锁死在以太坊中，被以太坊锁死的财产总额达到 2 亿美元，在 2017 年 11 月就有媒体爆料，以太坊的智能合约的误操作导致近 3 亿美元资金被永久冻结在以太坊中。在伦敦大学计算机科学系的一次最新调查中，对近 100 万份智能合约进行分析，有将近 3 万多份智能合约是很容易受到攻击的，另外该调查又对 3759 份智能合约抽样调查，其中有 89%的合约是含有漏洞的。

另外，目前智能合约的代码的执行与区块链的强耦合模式也对区块链的性能造成严重的影响，使得现有区块链技术不得不应对各种扩容方案。

让我们的思路再次回到数字合约本身要解决的问题上来，这里选取一个多人参与公平博弈游戏的合约的例子。想象一下，Alice 和 Bob 决定玩牌，Bob 拿出一副牌，先洗牌后发牌，一半发给 Alice 一半发给自己（避免使用整副牌），然后按照游戏合约的规则，轮流进行出牌

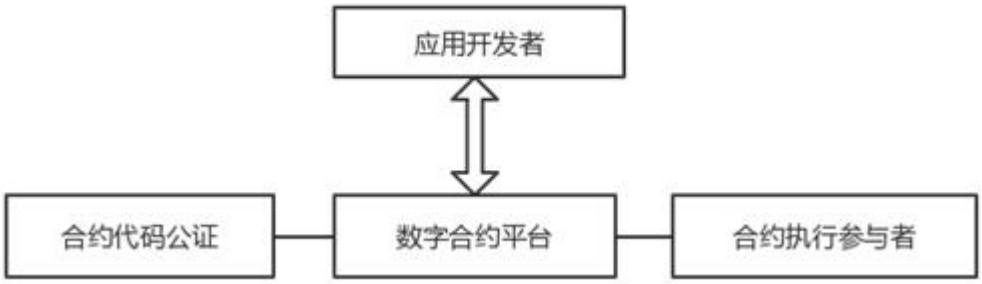
或比牌的操作，直到游戏结束。在以太坊上要实现这个合约就是创建一个实现玩牌规则的智能合约，跟踪每个玩家的操作，每次当一个玩家做一次操作的时候，他会向智能合约发起一次交易，然后由矿工在生成区块的时候执行这次操作。这是可行的，但是效率极其低下而且每次操作的确认时间非常长，同时为了完成整个游戏，他们不得不多次支付昂贵的 gas。

在 GFCC 公链中，我们设计了一种链外可信合约的机制，而这样的一个系统，让 Alice 和 Bob 在执行合约过程中尽可能少地在链上进行操作，最终在合约执行完成或在合约执行的关键节点处才将重要数据记录到链上。这也就是说，我们将链上合约代码的执行权限开放给合约的参与者在外部进行写作完成，链上只保留数据的存储和数据的验证功能。这样的设计直接大幅度地降低了区块链的负载。

因为合约的执行只在合约的参与方在链外进行，避免了全局的消息广播；同时合约的数据、代码执行与区块链的交易行为彻底解耦，这也大大地拓展了智能合约的应用边界。

7.1 合约的设计架构

基于以上的分析，GFCC 公链在最底层，提供了一套智能合约执行的虚拟机环境，它会根据上层的业务需求自动匹配对应的密码学组件和基础的网络通信模式，再在其上构建起一套易用的可形式化验证的函数式编程语言，让业务场景开发者像开发简单的单机应用一样的去开发去中心化的应用逻辑，而且应用开发者只需要关注自己的业务逻辑而无需关注底层的密码安全技术以及复杂的 P2P 网络架构。另外在底层的区块链上，我们会提供一套完整的数据模型和数据读写及数据验证方案，在智能合约的底层完成对数据安全性和正确性进行校验。



其核心特征主要包括但不限于以下几个方面：

A 解耦了数字合约的执行与主链的关系，消除了网络处理的瓶颈，同时也大大地提高了应用的可扩展性及应用边界。

B 通过引入密码学底层算法及可验证的合约执行虚拟机环境，链上保留了合约通道建立及初始化安全参数的分配权限，保证了合约执行的参与节点无法篡改数据和无法修改合约的执行过程。真正做到了过程的安全性。

C 由于合约通道具有隔离性的特征，保证了各个业务及相同业务不同的执行节点具有隔离的安全性。

D 通过在合约中引入角色自定义的机制，与现实世界中的个人、组织、权限等等形成一种映射关系，让每个参与执行合约的节点具有了现实世界中合约的属性。

在数据存储方面，我们采用一种支持事务性的 Key-Value 分布式数据库，提供业务最基本的数据读写功能。独立于每次数据读写操作的时候，我们会为每次合约执行时针对数据的增、删、查、改记录以类似于传统加密数字货币交易的形式保存到区块链上，这样在数据层面就做到了数据操作的可溯源性。通过公开区块链账本的形式，任何个人或任何组织都能以自己拥有的权限对数据进行事后验证。

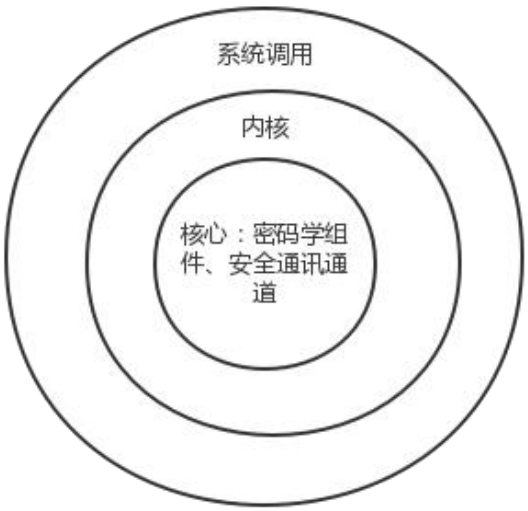
需要注意的是，为了保证数据读写的一致性，如果事务是为某个键多次写入，则只保留最后一次写入的值；即使在事务读取结果发出之前更新了键值，也会返回事务读取已提交状态的值。另外这里有一个非常重要的技巧就是，我们在设计键的时候，充分利用每个合约通道的

唯一性，保证在同时写入相同的键的可能性几乎为零。

7.2 合约的运行环境

功能上看，首先由应用开发者基于业务需求编写对应的数字合约执行流程代码，测试通过后发布到数字合约平台。由于数字合约的代码是写到区块链上的，任何个人或组织都有权限查看合约的源代码，对代码的合理性和公平性做正确的人工审查，特别是作为智能合约的参与方有权利对代码进行审核。合约执行参与者作为合约执行的主体，会选择合约中指定的合适的角色参与合约的执行。

由于 GFCC 公链的数字合约的代码是脱离于主链运行，为了保证安全性，核心合约层提供了一个智能合约的虚拟机执行环境，我们将其命名为 FraVM，该虚拟机环境可以为应用层提供消息通讯框架和逻辑控制。FraVM 虚拟机内部本身具有图灵完备性，可以实现任意逻辑，同时具有高度的确定性，可保障在所有参与节点上实现“输入和输出一致”。FraVM 的结构图如下



FraVM 虚拟机环境的在设计上分为三个层次，在核心层提供基础的安全通讯服务，在内核

层提供一套类似于 javascript 语言的虚拟执行环境，该层会读取合约代码并执行安全计算及正确性验证，在上层，应用开发者利用内核提供的角色定义、轮次代码执行切换功能定义相应的逻辑功能。

八、通证发行机制

此次 GFCC 基金会发起的区块链项目简称“GFCC”，发行总量恒定为 10 亿个，且保证永不增发。

8.1 通证介绍

GFCC 作为 GFCC 公链平台的治理通证，除了少量的预挖之外，完全由矿工节点通过容量证明的方式挖矿产出，具体挖矿参数如下：

出块时间：1 分钟

挖矿总量：950, 000, 000

减半周期：4 年

初始区块奖励：7.5

8.1 通证分配

GFCC 是一个创新型公链，其激励通证名为 GFCC，GFCC 发行总量 10 亿枚，无 ICO，GFCC 整体分布情况如下：

比例	**数量**	**分配方式/用途**	**备注**

5%	50M	项目团队	项目团队激励
95%	950M	矿工产出	持续挖矿产出，4 年减半

九、治理架构

9.1 GFCC 基金会

GFCC 基金会位于新加坡，属于一种非盈利性质的公司，符合 Blockchain 去中心的这一重要特质。新加坡是亚洲的 Blockchain 项目中心，可以出具法律意见书，项目在新加坡法律的框架下合规运营，合法合理。项目选择注册于新加坡，有利于项目的顺利运作。

9.3 技术团队

GFCC 项目核心技术和设计人员由美国麻省理工学院，哈佛大学，香港大学等多家国际知名学府的高端人才构成，致力于互联网软件及硬件的学术交流，人工智能，大数据，区块链领域的技术研发工作，先后为技术领域提供了数千项创新技术及论文。技术研发及制作团队，由实验室与来自全球多家制作机构联合组成.，1000+工程师团队，技术实力雄厚。

10、风险提示和免责申明

10.1 免责申明

该文档只用于传达信息之用途，并不构成投资意见。任何类似的提议或征价将在一个可信任的条款下并在可应用的证券法和其它相关法律允许下进行，以上信息或分析不构成投资决策，或具体建议。本文档不构成任何关于证券形式的投资建议，投资意向或教唆投资。本文档不组成也不理解为提供任何买卖行为，或任何邀请买卖任何形式证券的行为，也不是任何形式上的合约或者承诺。GFCC 基金会明确表示相关意向用户明确了解 GFCC 币的风险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意个人为此承担一切相应结果或后果。基金会明确表示不承担任何参与 GFCC 币项目造成的直接或间接的损失，包括：

1. 因为用户交易操作带来的经济损失。

2. 由个人理解产生的任何错误、疏忽或者不准确信息。

3. 个人交易各类区块链资产带来的损失及由此导致的任何行为。

GFCC 作为 GFCC 公链的通证，不是一种投资工具。我们无法保证 GFCC 一定会增值，在某种情况下也有价值下降的可能，没有正确使用其 GFCC 币的人有可能失去使用 GFCC 币的权利。GFCC 币不是一种所有权或控制权，控制 GFCC 币并不代表对 GFCC 公链的所有权，决策权。 GFCC 币并不授予任何个人，任何组织参与、控制 GFCC 公链决策的权利。

10.2 风险提示

任何一个行业都存在激烈的竞争，没有哪一家企业是不可替代的，没有哪一家企业的发展是一帆风顺的。竞争将是残酷的，但在这个时代，任何好的概念，创业公司，甚至是成熟的公司都会面临竞争的风险。我们全体员工一定会努力为目标奋斗，但是基金会不能 100%保

证企业能按照规划目标完成任务。当然购买数字货币是一种高风险的投资方式，请投资者谨慎购买，并注意投资风险。