THE KAi Coin WHITE PAPER

区块链与文化相融合
改变货币价值的加密货币平台

www.kaicoin.io

原始版本 1.0 ： 2017-05-01
最新版本 1.2 ： 2017-08-18

目　　录

1. 概要

“KAi Coin”是一款由韩国投资者协会投资而开发成的虚拟货币（加密货币），旨在扩大投资者协会成员的利益，用作韩国及海外关联公司对有关资讯的支付手段。KAi Coin通过改进并完善比特币与以太坊的技术缺点，将加密及传输速度提升了10倍以上，从而被评为以安全为中心的加密货币。由于KAi Coin总量（总发行量）限定为21亿KAI（“KAI”为Kai Coin的货币单位），随着其在世界范围内的普及和推广，货币本身的稀缺性会日益凸显，币值也自然会随之提升。

同时，已搭建好可用于移动（手机）游戏、网上购物商城、虚拟现实（VR）内容等的使用环境及系统，今后，KAi Coin的使用环境有望迅猛扩展。

此外，还将通过搭建无懈可击的安全系统来实现收益，并自主运行综合交易系统，以保障KAi Coin、比特币、以太坊乃至世界著名的虚拟货币（Alctoin，又称为“竞争币”）之间安全交易。

2. 背景

区块链由“中本聪”（Satoshi Nakamoto）于2009年诞生为比特币的核心技术。

比特币为解决双重支付（双花）问题而采用区块链。目前，区块链之所以作为一种金融交易总账，用于公开记录个人货币传输信息，其根本原因就在于此。之后，基于区块链技术的虚拟货币层出不穷，至今约有800种加密货币相互之间展开竞争，且已在世界范围内广泛使用。

同时，许多企业及银行纷纷引进联合（行业）区块链（Consortium BlockChains)，加大对区块链技术的投资力度。

区块链已受到各行各业的广泛关注和重视，主要由拟使用并管理货币、金融商品、服务、物流信息、财产所有权、知识产权、个人信息及各种数字财产的行业进行研究和开发。此外，由维塔里克·布特林（Vitalik Buterin）诞生于2014年7月的以太坊，则以提供“可用于实现任意状态转换函数的合约”——智能合约（Smart Contract）功能的区块链为核心技术。就这种基于智能合约的区块链而言，最大目标在于让用户能够将所有类型的合约（程序）用在区块链上，智能合约可用于去中心化市场、货币交易平台等。

然而，这里还存在比特币所包含的问题——传输速度延时（支付/汇款）、区块容量（1MB）较小，以及以太坊本身所包含的安全隐患（DAO）等。

目前，第四代货币——加密货币已在全球范围内受到广泛关注和重视，人们对更安全、更方便的货币的需求日益高涨。KAi Coin通过改善比特币及以太坊所包含的缺点，提升了易用性及安全性，尤其是，着重于以基于韩国文化的电子商务为中心的区块链技术，大幅提高了用户方便性及收益性。

3. GSChain介绍

“GSChain”是一种“按需定制”的平台，可以在不同组织之间形成并分享特定区块链。

GSChain通过采用使用方便的软件包，保护隐私并管制权限，由此解决在区块链技术推广到金融圈方面所存在的难题。GSChain是一种由Bitcoin core（比特币核心钱包）软件衍生而成

的，不仅支持Windows、Linux、Mac等多种操作系统，也支持简单的应用程序编程接口（API）及命令行接口（CLI）。下面将介绍GSChain的原始版本（公开）及其特点。

3-1. 私有区块链（private BlockChains）

GSChain通过对用户权限进行综合管理，提出针对“开采”（相当于比特币的“挖矿”）、隐私权、开放性等问题的解决方案。GSChain核心目的可分为如下三点。

1) 只以被选定的参与者为对象显示区块链活动；
2) 引入在允许交易方面所需的控制方法；
3) 不会产生涉及PoW（工作量证明）等的相关费用，而可保障安全开采。

若实现区块链的“私有化”，相关区块链的参与者可以调整区块的最大容量，由此可容易解决区块扩展问题。同时，这属于一种封闭性系统，只有与参与者有关的交易才会产生。

所有的加密货币都采用公钥加密方式（public key cryptography）来管理用户身份及安全。加密货币的用户各自任意生成私钥，并不向其他任何参与者公开。各个私钥有着从数学上相连的公开地址，以此替代领取资金的身份。若资金汇至公开地址，只有持有私钥才能将相关交易“成交”。这就意味着访问私钥直接关系到拥有相关钥匙所保护的资金。

这种加密方式让用户能对相关消息进行签名，以控制对资金的访问权限，并证明用户持有与特定地址有关的私钥。得益于这种特点，GSChain只允许属于授权列表（允许访问名录）中的用户才能访问相关区块链。如下所述，两个区块链节点相连时，即会经过相互“确认”的流程。

区块链的确认（握手）流程

1) 每个节点在授权的列表上呈现自己身份（公钥）作为公开地址；
2) 每个节点确认（验证）对方地址是否在各自授权的列表上；
3) 每个节点给对方发送一个询问消息（challenge message）。
4) 每个节点对其所收到的询问消息进行签名（Signature）并回复，证明其拥有与现有的公开地址相关的私钥。

若任何一个节点没有满足条件的结果，系统就会强制终止P2P（点对点）连接。

将权限与公开地址相连的原则可在网络上适用于其他功能。例如，可以将汇款/收款交易权限控制在特定列表上，这是因为在交易记录中载明着汇款人及收款人的地址。因为会有汇款人/收款人为两名以上的情况，只有属于相关交易的汇款人与收款人都在授权列表上，才能允许相关交易。当然可以完全公开地读取区块链，也可以仅限制交易功能。最后，可以通过在开采者（相当于比特币的“矿工”）所加入到区块中的Coinbase（币基）交易上添加签名栏，相同地限制在GSChain上开采。这在防止少数用户掌握私有区块链（私有链）方面起到核心作用，具体内容将在后面提到。

GSChain权限

GSChain通过采用包括特定元数据在内的网络交易方式，对所有的权限予以批准和取消。“创

世（genesis）”区块开采者将拥有一切权限，包括可管理其他用户权限的管理者权限。管理者通过利用交易输出值所包含之用户地址及标明拟授予用户权限的元数据，授予其他用户有关权限。更改其他用户的管理者权限及开采权限时，将会有附加限制。就是说，现有管理者须对更改内容表决同意与否，征得最小比例以上的同意才可更改权限。表决内容及其结果将由相关管理者通过另一笔交易进行注册，对此达成共识（协商好）时才可正常反映更改内容。当创建区块链之时，部分区块会构成“设置阶段”。此时，可由一名管理者跳过上面所提到的表决流程。
今后，未来版本可以在GSChain上反映“超级管理者”，超级管理者有权独自批准/取消权限。

因为权限更改内容储存于交易内部元数据中，相关内容将快速广播到网络中所有节点，并对当前状态达成共识。但因为采用分布式网络，不同节点在接收到相关交易信息的时间上可能存在先后差别。例如，如果因为付款交易的有效性尚未广播至全网，导致其权限更改内容未能正确反映到每个节点上，这会引起致命性后果——有的节点批准支付，有的节点拒绝支付。

这种因时间序列所致的问题，相关交易在区块链中得到验证（确认）后即可解决，随后将决定最终顺序。因为交易按区块链的顺序进行“重放”，区块中的每一笔交易都须依据上一个用户的权限保持有效。若任何一笔区块中的交易无效，则视为整个区块都无效。即使区块有效，只有在相关区块的交易所定义的授权列表（允许名录）上存在开采者，才能视为有效。

但就访问权限而言，因为其与区块链内容无关，而不受这种权限管理体系的限制。不过，对特定地址的访问权限被取消时，每个节点都在响应验证过程中，将与使用相关地址的节点之间断开连接。

为方便起见，以固定范围内的区块号为对象，可以批准有限制的临时权限。这种基于临时权限的交易，其有效性仅限于指定范围内的区块号。若要修改权限，就须由数量充足的管理者正确选定符合相关用户及权限的区块范围，才能视为达成共识。由此可以提高网络透明性，也可以减轻对逐一取消有效期届满的临时权限的负担。

为了使区块链真正成为“私有化”网络，所有地址都在区块链上得以批准，此时，至少一名以上管理者必须知悉相关地址所有者（用户）的身份。然而，大多数参与者则无需相互知道对方身份。“peer-to-peer”（点对点）交易是区块链的主要功能之一，主要对两种形式的代币（Token）进行交换。若地址的匿名性得到保障，就可以在不知对方身份的状态下进行交易。金融机构通常以多个地址为基础对这种交易进行处理，只有指定负责人才能知道相应地址的所有者。

3-2. 在GSChain上开采（挖矿）

GSChain仅以可识别身份的当事人为对象提供开采权限，由此可以解决在私有区块链上开采权可能由一名开采者垄断的问题。就是说，限制同一个开采者可以在特定期间内产生的区块数量即可。

实现限制时所需的参数

mining diversity（限制为0 ≦ mining diversity ≦ 1）

利用参数验证区块有效性

1) 以区块中的交易所定义的内容为准，按顺序适用所有的权限变更；
2) 计算出经权限变更后获得允许的开采者数量；
3) 将开采者数量与开采多样性参数值（mining diversity parameter）相乘而得出的数值四舍五入后，得出spacing值；
4) 若相关区块的开采者曾经采过spacing-1区块，相应区块则视为无效。

通过应用“round-robin”方式（轮询调度算法）获准的开采者，只有轮流产生区块才能形成有效的区块链。开采多样性参数由严格的模式方案（scheme）定义，这就意味着为掌控网络所需商定的获准开采者比例。当参数值为“1”时，所有的获准开采者都被纳入循环中；当参数值为“0”时，则意味着不受任何限制。一般来讲，参数值越大，网络越安全。但若其过度靠近“1”，部分开采者不做活动时，区块链本身可能暂时停止。因此，建议参数值设为中间值——“0.75”。每个节点不会再开采以前的“spacing - 1”区块，以节省资源。

若以多样性参数予以限制，不仅可以预防恶意活动，也在因通讯中断等原因而造成网络暂时断开时会有所帮助。此时，被断开的网络区域中的一个节点，无法查看其它区域中的交易或区块，因此而会在区块链上产生“分叉”（fork）。网络得以恢复后，将以最长链的分叉为准在全球范围内达成共识。就是说，通过采用多样性限制方式，可以保障最长区块链属于多数获准开采者所属的区域中。此时，其他区域中的区块链即会冻结。

私有区块链的有用性

为何非要使用私有区块链，如使用中心化数据库如何？　因为中心化数据库本身也能够处理一系列流程，包括接受交易、解决争议，以及与数据库状态相关的查询响应等。私有区块链的必要性及有用性如下：

1) 在区块链上，每个参与者可以通过利用私钥来完全控制自己的资产。开采者也无法用其他参与者的资产来产生任何一笔交易。
2) 因为数据库控制权分布于多数参与者之中，特定个人或少数群组无法独自判断有无交易。
3) 与中心化数据库相比，区块链保持着更稳定的状态。即使一个服务器消失或故障，也不会影响全网中的交易。

在基于权限的开采中，工作量证明（PoW）如何？
比特币通过工作量证明机制，增加开采所需的运算难度（即，增加所需成本），由此保证开采多样性。
相反，私有区块链则通过采用更简单的方式保证开采多样性，因此，为工作量证明所需的工作不过是一种形式而已。实际上，GSChain的原始版本仍采用比特币PoW机制，以限制每个节点的区块生成率并使其随机化。但这也不能当成区块链的安全装置。

在GSChain区块链上，交易手续费及区块奖励设置为“0”（默认值）。若区块开采费用极小以至可以忽略不计，开采者也无需接受其他奖励，而会为从区块链本身的灵活功能中获得利益而进行开采。然而，开采者可能以网络参与者为对象征收固定的年会费，此时，不是通过区块链方式，而是通过“制度圈”支付方式来付款。假如说区块链的唯一目标是给代币化资产提供交

易，那么，相关网络的加密货币可以仅仅视为简单的技术创新。不过，在交易的稀缺性凸显的情况下，GSChain也可将加密货币设置为区块奖励或最小交易手续费及交易量等。此时，参与者需要从开采者中购买加密货币，可采用代币化资产等作为购买手段。

3-3. 驱动多个区块链（多链）

与支持单个区块链的比特币核心钱包（Bitcoin Core）不同，在GSChain上可以同时构建并运行多个区块链。同时，私有区块链是可以由系统管理者构建并运行的，而不是仅限于特定开发者，从这一点上看，GSChain对于有关机构来说也是更方便、更有效的区块链。比方说，其类似于Oracle、SQL Server等关系数据库管理系统（RDBMS）可以用几个简单的SQL命令语句来创建并使用数据库。同时，支持多个区块链的另一个优点是，可以由服务器与其他区块链的活动相连。例如，若资金汇至特定区块链上，就可以让其再汇至其他区块链上。

在GSChain上可由用户设置的区块链参数

1. 区块链协议	可设置为靠近于私有区块链或原始比特币。
2. 各个区块的目标时间	可设置为1分钟等。
3. 批准权限类型	可设置为谁都能访问或仅限部分收发。
4. 开采多样性参数（mining diversity）	例）0.75
5. 创建/删除管理者及开采者时所需的共识水平，以及不受这种限制的设置阶段及期间	仅限于私有区块链。
6. 开采奖励	例）每个区块以50个为单位， 设置为以每21万区块为准减半。
7 为P2P连接所需的IP端口及JSON-RPC API	例）8571、8570
8. 允许的交易类型	例）pay-to-address、pay-to-multisig、 Pay-to-script-hash
9. 区块最大容量	例）1MB
10. 每笔交易的最大元数据	例）4096字节

可以在一个服务器上激活多个区块链，让不同的区块链拥有不同的名称及设置文件。要创建新的区块链，就需要设置两个条件。

1)用户选择区块链名称后，GSChain将创建具有默认值的设置文件。该文件可以由用户修改，通常保持基本设置条件（默认值）。
2)用户执行区块链后，GSChain将开采创世区块并授予其开采者（创世区块开采者）所有的用户权限。此时，将有关创世区块的详情及相关区块链的参数哈希（hash，又称为“散列”）储存于设置文件中，以备不测。

GSChain流程

首次执行后，区块链将由一个节点运行。为了添加节点，GSChain需要在其他计算机上用三个参数来执行：（1）目的地区块链名称；(2) IP端口号；(3) 现有节点的IP地址

为方便起见，将该信息以“节点地址”形式捆绑而使用。例）gschain@127.0.0.1:0000.
因为采用私有网络，起初新一个节点因尚无访问权限而无法连接到相关网络。GSChain将显示包括新节点所自主生成的公开地址在内的消息，须发送该地址给管理者。管理者用简单的命令语句来产生交易并授予新节点对相关地址的访问权限。新节点由此可以访问相关地址，实际访问时会自动下载已定义区块链特性的设置文件。下次以相同区块链再次访问时，只需区块链名称，经过响应验证流程，可以确认两个节点是否使用相同参数。

GSChain待改进事项

今后必须改进的事项是，让区块链在运行中通过可靠的管理者发行的特定交易来修改部分参数。例如，在网络使用率增加的情况下，为了好好控制并处理交易量，可以扩大区块最大容量。为此，就需要考虑网络上的每个节点的运算能力及水平。

3-4. 复合货币区块链

如上所述，若使用CoinSpark或Counterparty等代币化协议，就可以与比特币本身的货币一同在比特币区块链上发行第三方资产并对此进行交易。这种方法无需另行修改，即可适用于在GSChain上形成的私有区块链上。然而，在采用私有协议的区块链上，通过将支持第三方资产的功能反映到区块链规则上，可以进一步完善。

在比特币机制上，将存储于每笔交易结果值中的比特币数量进行编码（符号化）。若在输出值中编码的比特币总量小于反映在输入值中的比特币数量，相关交易将在相关网络上视为无效，从而其不会在区块链上验证，也不会广播到相关区块链。因为网络上的每个节点会跟踪未耗尽的交易输出值中的比特币，可以经过这种验证流程。因此，用户通过确认在网络或区块链上是否进行交易，可以判断出储存于交易数据中的比特币数量是正确的。得益于此，“SPV轻钱包”（simple payment verification，简单支付验证）可以与网络进行安全交易，也无需将全部区块链储存到用户计算机中。

“代币化”的缺点

在比特币机制上，因资产“代币化”所致的问题是，用于对外部资产进行编码的元数据不会经过网络级验证流程，从而无法对比特币本身进行验证。例如，假设“ABC”银行发行了象征着美元的代币（Token）。恶意用户可能创建一笔带有输出值为100 ABC美元的元数据的交易，即使实际上这笔交易的输入值中却无ABC美元。这种交易可能在比特币网络上视为有效，且可以在区块链上得以验证。其原因在于：第一、比特币节点无法读取该元数据；第二、比特币节点不会跟踪ABC美元。

因此，与比特币相比，代币化资产在比特币区块链上被看成是个“第二通用货币”。要确定是否存在代币化资产，就需要查看从头到尾的全部交易记录，即从最初创建相关代币的交易到影响相关代币的所有交易。这可以通过“向前”（forwards）方式有效计算。就是说，每当发生新一笔交易时就进行检核即可。然而，即使如此，也需要整个网络节点，并且，代币化协议不宜与轻钱包一起使用。

GSChain为了解决这个问题，将所有资产的标识符（identifier）及数量都编码到每笔交易的输出值中。此时，使用比特币脚本语言所提供的扩展名（extension）。由此可以扩展交易验

证规则，从而能够确认交易输出值中的所有资产总量是否与输入值相同。GSChain根据与比特币相比更严格的验证标准来确认输入值与输出值是否相同。在比特币机制上，若输出值小于输入值则视为有效，此时所产生的差额就用作开采手续费。当然，在使用这种方法之前，需要允许相关区块链通过带有特殊元数据的首笔交易来生成新资产。GSChain根据这种首笔交易在区块链中产生于何处，自动安排对新资产的标识符，将其与用户自定义标识符一起使用。

GSChain的授权系统还可用于控制资产形成权。同时，未来版本可以引入按资产设置权限的方式，由此可以按资产设置管理者、获准发送人/接收人等。这是以简洁性为由未纳入到GSChain原始版本中的功能，但在已被反映的规则基础上，只要通过简单扩展即可添加该功能。

3-5. 比特币与私有区块链之间转换

上世纪90年代互联网席卷全球，数以百万计的人们面临着新的范式。公司希望将这个创新型技术应用到组织内部，但当时许多公司还认为互联网在隐私、可靠性、容量等方面有很多不到位之处。因此，许多公司搭建了将互联网内在化的“内联网”（Intranet，又称为“企业内部网”）。内联网采用了相同于互联网的基础设施及技术，但完全可以由公司控制。
自那以后过了20多年，互联网现已成为可将大容量信息在全球范围内稳定传输的网络，使得许多公司选择并应用VPN（虚拟专用网络）。VPN基本上采用互联网技术，但同时采用对相关组织的通讯内容进行加密的方式，因此，即使通过公共通信网络广播也可稳定保持安全。就是说，VPN不仅能让公司享受互联网，也能防止有关数据被泄露到外部。

比特币区块链及私有区块链也现正进行类似流程。从企业方面看，比特币网络是一个尚未征服的领域，因为容量有限，也无法预测长期交易成本。尤其是，比特币开采权（挖矿权）主要由不特定多数人管制，其中大多数人持有有悖于企业理念的思想，或来自于法制并不完善的国家。因此，对于金融机构来说，未来10年要有效使用这些技术，私有区块链就是一个更具魅力的选择。从现在开始20年内，如果比特币或其他区块链每月能以极低的成本处理数十亿笔交易，且由身份明确的大企业有效控制开采权，那么，届时比特币可以在金融机构之间的交易方面成为最具魅力的平台之一。同时，通过添加像VPN这样的薄型加密层，可以将相关机构的活动内容及记录从大多数网络参与者中隐蔽起来。

GSChain的概念设计旨在以多种方式保障私有区块链与比特币区块链之间进行双向转换。若有通过利用如下所提到的5)项功能进行资产代币化及消息传递（Messaging）的应用程序，可以在几乎没有更改代码的状态下，使比特币与私有区块链之间相互转换。

1) GSChain是基于比特币网络官方客户端——Bitcoin Core（比特币核心钱包）的衍生板而诞生的。代码更改经过本地化，可适用于比特币待改进事项。
2) GSChain采用类似于比特币协议、交易、区块链架构的平台。唯一的区别是两个节点首次连接时进行的响应验证流程。其他功能通过修改元数据及交易/区块的有效性规则来改变。
3) GSChain接口（命令行、API）可与Bitcoin Core接口完全兼容。同时，通过使用一些新的命令语句来添加其他功能。
4) GSChain只要通过在per-blockchain设置文件中简单地设置协议，即可在普通比特

币网络（或类似于比特币网络）上起到节点的作用。

5) GSChain的复合货币及消息传递（Messaging）功能非常类似于旨在改善比特币交易的 CoinSpark协议。

4. KAi Coin应用技术

4-1. 区块链方式

为了防止特定群体或组织抢占或垄断，公开透明地明示与预开采（pre-mined，相当于比特币的“预挖矿”）有关的信息及分享与否（是否回馈社会）。同时，KAi Coin通过采用公共区块链（Public BlockChain，又称为“公有链”）方式来共享奖励，以让每个人都可以参与开采工作（挖矿）。由此可以进一步提升相关加密货币系统的安全水平。

公共区块链又称为“非许可型总账”（Permissionless Ledger）。这意味着任何人都可以在未经事前许可的状态下，对区块链数据进行读取、写入和验证。KAi Coin也遵循这种方式。同时，每个人都可以下载区块链后，查看相关记录或通过加密签名方式参与记录。

参与者通过投票方式决定输入何种数据。赋予投票权的方式通常是根据投入的计算能力（成比例）而不是根据节点数量。然而，KAi Coin通过保障开采多样性，防止投票权由计算能力强的节点垄断。由此，保障尽量多的节点开采成功。

4-2. 区块时间与区块容量

从一开始，KAi Coin拥有3000-4000名用户（会员），而交易速度及安全最为重要。因此，通过对区块容量进行动态分配（最小值：4千字节，最大值：2048千字节），有效提高节点的传输速度，保持稳定的传输速度。

同时，通过将区块时间指定为60秒钟，可以在平均60秒钟内对哈希（散列）区块头值进行链接（chaining），让用户可以体验比现有的比特币区块时间——10分钟快于10倍的高级SHA256哈希技术。

这两点有助于防止下一代区块链货币的最大问题即“交易失败”及“支付延迟”，也有利于保障交易安全以至达到现有的比特币安全水平。

此外，对于当前颇受业内关注的热门话题——区块最大容量，通过将其指定为被认为最有效的2048千字节，可以解决以前受限于区块容量的问题。

4-3. 多重签名脚本

“Pay to Script Hash”（P2SH，支付到脚本哈希）让用户更容易使用同时需要两个签名的加密方式。通过使用P2SH，可以在复杂的锁定脚本上以数字指纹替代加密哈希值，也可以在系统上选择有效的交易结构，还包括可减少相关交易规模的优点。

4-4. 半衰期

以半衰期1年为准，提供可以共100年开采的公开开采系统。据预测，以区块时间1分钟为准，共3年有望形成约157.68万个区块。这是为了给开采者提供更好的开采环境。同时，考虑到最初发行量——21亿KAI，认为若未能提供充足的开采机会、难度及期限，则无法稳定保持以安全为中心的区块链生态系统。

营造更好的开采环境，就是忠实履行区块链技术宗旨的第一步。

4-5. KAi Coin技术参数

- 哈希算法（Hash Algorithm）：高级SHA256
- 总发行量：21亿KAi Coin
- 发行方式：开采（Mining）
- 区块时间：60秒钟
- 区块容量：2048千字节

5. KAi Coin介绍

5-1. 目的

KAi Coin是以KAii协会成员对改善一直有害加密货币市场的陈旧环境的愿望为基础开发而成的。KAi Coin是一款满足用户对安全、速度及透明度的需求的“加密货币”，同时也是作为开采型加密货币，通过采用高级SHA256方式，改善了比特币缺点——支付延迟及安全问题。尤其是，KAi Coin所采用的区块链是针对电子商务方式开发而成的，由此给用户提供更方便、更经济的服务。

KAii协会的最终目标在于，与1万多家附属公司搭建相互有机结合的合作网络，为此，KAi Coin将发展成为有效的、安全的、不可或缺的支付手段。

KAi Coin不仅将成为在韩国乃至全球范围内通用的全球性货币，也将跃为以电子商务为中心的世界顶级加密货币。

同时，通过搭建基于区块链的系统，不仅将其适用于日常生活中的方方面面，也将具有韩国特色的内容及文化相融合，为实现社会文化的发展做出贡献，最终将成为在全球范围内通用的虚拟货币。

5-2. 应用平台

随着信息通信技术的快速发展，人们仅靠过去的方式则难以在当前激烈的竞争环境中继续生存下去。“平台”在这种时代需求下应运而生，与时俱进，如今已成为左右企业成败的关键因素。

在加密货币市场，“基于平台”这一概念最初由维塔里克·布特林（Vitalik Buterin）于2015年开发的以太坊诞生。这从概念上有别于只具货币功能的比特币，今后，像以太坊这样基于平台的加密机制将会引领第四次工业革命时代的大趋势。

KAi Coin也是基于平台的加密货币机制，韩国投资者协会将以此为基础和支撑，在多个商业领域及社会贡献领域开展多种多样的活动。

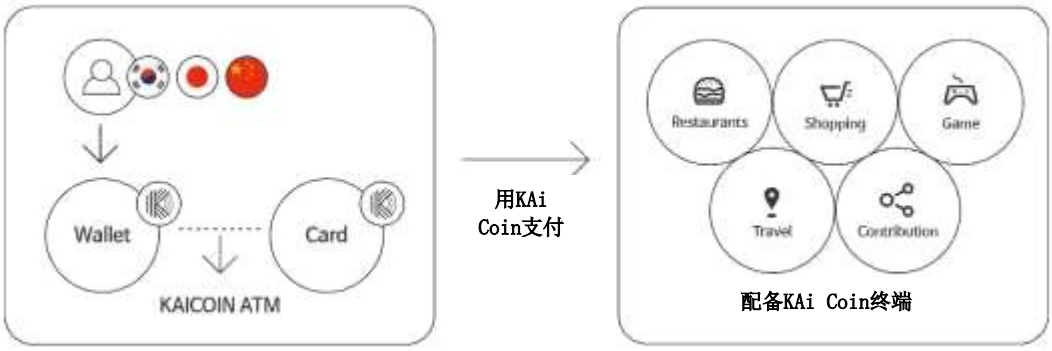
社会	- 通过共享区块链技术扩展社会基础设施。 - 通过构建社会贡献平台，支持非营利活动，为NGO团体提供公开透明的财政支持。
文化	- 基于K-Culture（韩国特色文化）内容，已搭建好针对中国、日本市场的营销平台。 - 通过应用分布式系统，将适用范围扩展到虚拟现实内容、移动视频导航等领域。 - 确保餐厅、糕饼店、旅行社、医院等实体（线下）加盟店。 - 扩大对韩国/海外网上购物商城的支持。 - 支持网络游戏内道具交易。
经济	- 建立KAi Coin综合交易所“KAIREX”。 - 通过自动存取款机（ATM）利用KAi Coin。 - KAi Coin登载至国际交易所。

5-3. 详细信息

- 正式名称：KAi Coin
- 货币单位：KAI
- 预售期间：（GMT+9）从2017年9月1日PM12:00至2017年10月31日PM11:59
- 单位价格：1500 KAI = 1 ETH
- 最小购买量：下限为150 KAI = 0.1 ETH
- 总供应量：200,000,000
- 交易货币：ETH
- 奖励：按周分等级提供
  （~第1周：20%，~第2周：15%，~第3周：10%，~第4周：5%，第5周~：0%）

总供应量 **2,100,000,000**	公开开采量	1,000,000,000
	预开采量	**1,100,000,000**
预开采量 **1,100,000,000**	韩国预售	600,000,000
	ICO	200,000,000
	社会贡献	100,000,000
	投资者持有量	100,000,000
	其他	100,000,000

5-4. 使用环境



5-4-1. 游戏

人类可以从游戏中获得的两个优点是“缓解压力”和“改善相关功能”。从缓解压力方面看，可以获得模拟竞争、代理满足及创作等机会；从改善功能方面看，有助于提高注意力（如围棋等）及程序记忆力（如针对老年人）等。

KAi Coin将作为一种“游戏币”广泛应用在游戏领域，并且，考虑到当前全球游戏市场的发展现状，对KAi Coin的需求有望在全球范围内持续增加。

5-4-2. 网上购物商城

“网上购物”是指用户通过互联网、PC通讯、手机（移动）等方式搜索并订购商品的行为。主

要支持信用卡支付、手机（移动）支付方式。目前，随着信息通信技术的发展，互联网用户人数的增加，以及易用性的提升，网上购物不断呈现猛增趋势，但同时存在个人信息泄露、支付系统不稳定等问题。这种现实要求加密货币逐渐成为新一种支付方式。
KAi Coin有望解决包括双重支付（双花）在内的支付系统不稳定、用户身份泄露、手续费过高等一些列问题。

5-4-3. 线上线下加盟店

“加盟店”是指属于一个企业联盟的店铺或商店，又被称为“连锁店”。“加盟”是指店铺与企业之间签署的一种营业合同，加盟店通过所属企业的品牌知名度，可以创造收益，也可以在经营管理等方面得到有关支持。
如今，加盟店数量呈现猛增之势，也有望持续增加。KAi Coin将与拥有著名品牌的企业合作，力争成为全国加盟店的支付方式。

5-4-4. 移动服务

- KAi Coin钱包

  一种可以领取KAi Coin并管理账户的电子钱包。

- KAIREX交易所

  一种可以用KAi Coin及其他虚拟货币来进行交易的交易所服务。

- 捐赠及其他

  一种可以搜索全球KAi Coin加盟店并提供礼品、支持/捐赠的服务。

6. 路线图

第1期 **（~2017.09）**	- 开发KAi Coin - 签订KAi Coin捐赠协议 - 完成ICO韩国预售 - 启动ICO全球预售 - 推出KAi Coin钱包
第2期 **（2017.10~12）**	- 启动KAi Coin交易所“KAIREX”服务 - 登载至国际交易所 - 扩大与供应商、PG企业的合作
第3期 **（2018）**	- KAi Coin与银行卡结合 - 与自动存取款机（ATM）联动，用KAi Coin简便支付 - 实现KAi Coin的“日常化”
第4期 **（2019）**	- 支持中国、日本支付系统 - 拥有1万多家实体（线下）加盟店 - 扩大以旅游产业为中心的支持力度 - 提供针对中国、日本游客的便利服务
第5期 **（2020~）**	- 力图进军东南亚及欧洲市场 - 定位为在全球范围内使用率高的代表性货币协议

7. 开发公司与合作公司

7-1. 韩国投资者协会

韩国投资者协会是一家成立于2010年12月的非营利组织，旨在支持经济教育、投资教育及天使投资俱乐部（Angel Investment Club），与合作公司开展股权捐赠活动，培养10万名健康投资者。

韩国投资者协会重点推进以下4大项目：
第一、金融教育项目。
通过韩国投资者协会资产管理学院的多种金融教育课程，为成员们提供有关资产管理及投资管理的教育，并为青少年提供经济教育服务。

第二、扶持投资俱乐部。
通过成立天使俱乐部（Angel Club）并予以经营支持，为成员们提供挖掘有价值的企业并进行投资的机会，从而协助成员们能够进行有效的资产管理。

第三、股权分享项目。
作为和谐相处的社会成员，以忠实践行企业的社会责任为目标，并以7000多家参与创新型社会贡献项目“股权分享活动”的企业为对象，建立资产分享合作企业网络。

最后，IT数字产业投资及经营项目。
韩国投资者协会迎来第四次工业革命时代的到来，为了适应世界对新型加密货币及其支付系统的需求，通过成立协会附属KAi Coin事业总部，基于韩国电子商务环境的考虑，成功研发了以安全性、孙素性、收益性为核心的KAi Coin。
KAi Coin不仅将由韩国投资者协会、成员乃至以下合作伙伴一起使用，还将作为全球性支付方式，广泛适用于游戏市场、网上购物商城、著名品牌加盟店等多个领域。
就加密货币而言，由于其“求过于供”的特征，必然会使货币价值大幅提升。这将给持有KAi Coin的成员带来巨大的经济效益。

7-2. 合作伙伴

KAii	WHITE STONE	Allreve	INCAPO
WOWZONE	PICK:LE 日本	PICK:LE 中国	Bit&Person
AllStarWORLD	Rosenbee Medical	烤牛肉专门店"味来屋"	金枪鱼专门店"大水金枪鱼"

※ 尚无官网的合作公司除外。
※ 您可以在主页上获取有关新关联企业的更多信息。

- KAii： http://www.kaii.or.kr/default/mindex.php
- Allreve： http://www.allreve.com/mshop/main.asp

- WOWZONE： http://wowzone.co.kr/mshop/main.asp
- PICK:LE 日本： http://ameblo.jp/pickle-japan
- PICK:LE 中国： http://weibo.com/u/5888766483?is_hot=1
- AllStarWORLD： http://www.allstarworld.co.kr
- Rosenbee Medical： http://www.rosenbee.com

8. 结论

韩国投资者协会附属KAi Coin事业总部自成立以来一直通过应用比特币的货币功能、以太坊的广泛平台基础，致力于开发进一步发展的下一代加密货币机制。值得关注的是，基于合理算法及实用区块链，研发了专业适用于广泛电子商务领域的技术，包括游戏、电子商务支付等。

KAi Coin开发组通过利用区块链技术确保了安全性及无缺性，并以此为基础搭建了基于区块链的系统，以使其广泛适用于日常生活中。

今后，KAi Coin将全力以赴把具有韩国特色的内容及文化相融合，为实现社会文化的发展做出贡献，最终将成为在全球范围内通用的虚拟货币。