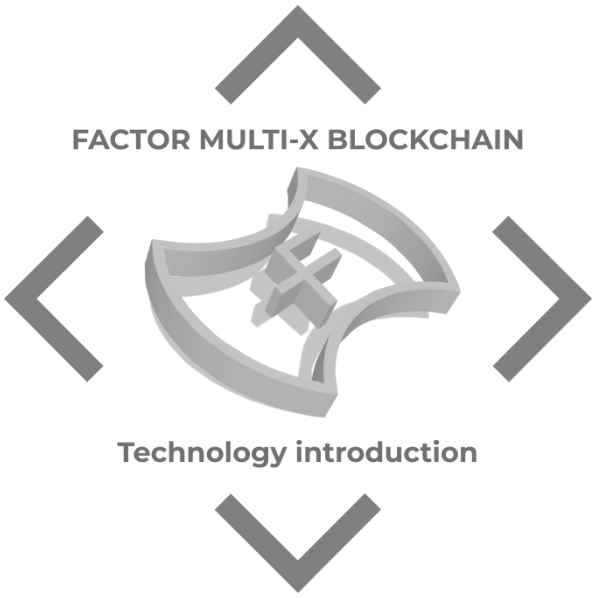
Factor Whitepaper



Version 0.1
Date updated: 06/05/2019

Factor Multi-X Blockchain
Company

导论

迄今为止‘技术’以多种多样的形态来发展。现在我们常用的网络也是之前以军事技术开始，活用在商业性活动等，之后现在一般人都能利用网络。技术是实现许多东西的驱动力，为了这些能够影响到许多人们的生活，最重要的就是活用这些技术来扩散到人们的实际生活中。在这些方面上块环链也是同样的。现在有许多人关心与块环链。排除中央集权性机关，给所有参与人赋予权限的个人主权主义的哲学原理，实现这些的 IT 技术，补偿体系，还有活用这些的商业性要素等都是依据区块链所展开的新典范。

但是,在区块链对我们生活的影响和变化可能性上放重点,观察目前的现状,不得不承认,区块链的发展阶段仍然处于"初级阶段"。 这是因为,尽管区块链技术不断发展,但新区块链开发者仍然使用依赖原有技术的方式，当面着高费用及多种多样问题。
此外,在各个区块链中需要解决的技术性问题依然存在,其实在现实上许多区块链在创意或概念水平上都是被提案开发。

Factor 区块链为解决这些问题进行了开发与研究,解决了现有的 orakle **问题及 TPS 速度,区块链的扩展性等课题**,为今后的次时代网络提供可应用的区块链。 **Factor 区块链**的目的是与现有的区块链体制进行整合, 如果现有的区块链能够成为一个区块链,则将解决区块链目前存在的 orakle 问题,或在 TPS 速度,扩展性,互换性及应用在实际生态系统中可能会出现的多种多样问题。

应用区块链的技术的使用不仅仅是用于金融,而在即将到来的**第四次产业革命**将要带来的产业生态系统中,发挥高速度,互换性和扩展性以及无限的应用价值，活用为革新性用途。 更进一步,我们 Factor 区块链技术部确信,这将成为在智能手机,家电,汽车,智能家居,气象观测,贸易等多个领域改变经济生态根基的创新契机。

Factor MX 区块链不仅连接现有的区块链,还会解决现存的**技术困难,过度的费用,程序开发语言的不一致**以及无法与现有程序互换及使用等问题。而且为了区块链的生活化，不断进行开发，且付出努力。 Factor MX 区块链将以区块链的多彩适用可能性为基础,根据新剧本和应用的要求,将会持续增加必要的模块和协议。

区块链是通过 **Factor MX 区块链重新定义，**与区块链我们即将面临的未来是依据 **Factor MX 区块链实现的。**

Index

1. 构造及设计

1 - 1 设计框架

Factor 区块链是通过应用 MX (Multi-X) 区块链来支持多重系统框架分散元账系统。这是通过 MX 区块链所拥有的 26 个以上的 Factor 专利散列来提高速度，扩张性，互换性，且通过链接各个散列连接到区块内，因此可以与所有区块链互换，而且扩张性优秀提供多种多样的功能。通过这些可以应用到许多平台上，而且通过 MXnode, Seed node, Masternode, Nomal node, Pos 的 spread 连接方式,

Pow 的算力的加速方式提供卓越的速度。而且 MX 节点系统是起着提高保安及速度的作用，这是选择 21BP 一样，是在原有系统上提高速度而所试图的方案，把在之前阶段上所应用的散列形成的区块链按照下列形成节点后被使用。Dapp 使用者可使用这些功能，以低费用，高效率开发可互换的软件，而且 Factor 的 Bootstrap 技术是可提前下载原有的分散账簿，因此确认引导法 SHA256Checksum 后进行下载，具有卓越的保安方式，不需要进行整体同步化过程，可直接加快速度。应用这些不但可以收容次世代网络所需，而且修行区块链能够带来的未来创新性作用，统合原有区块链的方式连接成一个区块链。

1)在不包含被参照的区块的复刻中防止生成交易。

2)**含有 26 种以上收到专利的散列算法**，具有卓越的**速度，保安性，扩张性。**

3) 通知特定用户和股份在特定复刻中。

4)可使用特定用户的 POS 协议算法。

5)可使用特定用户的 POW 协议算法。

6)MX Seed node 技术是具有着先带来特定指定节点来连接的功能。

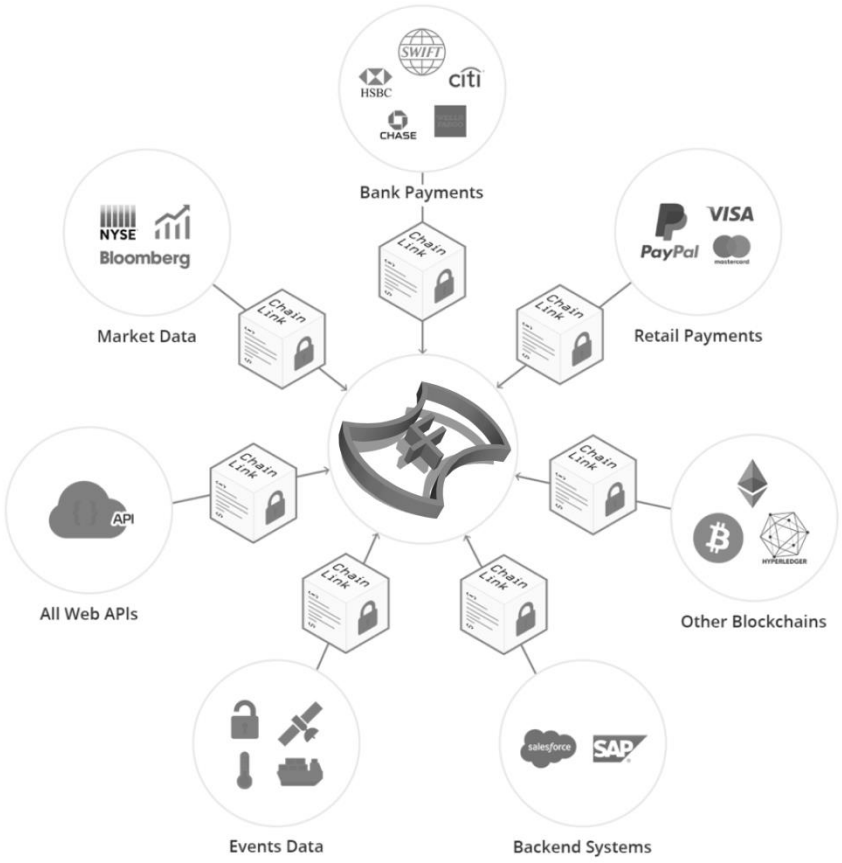
7)MX Masternode 技术是具有网络的连接维持性，维持及提高保安，速度等功能。

8)1 是与协议算法 POS，POW 互换的方式来运营且连接与 oracle 区间。与 oracle 区间联动时启动为互换 POS，POW 和多种多样协议算法的方式。

9)Dapp 使用者是区分为原有用户和新用户，能够使用上述功能，原有的其它平台用户可以利用 Factor 的网络连接 Dapp。

1 - 2 应用分散元账

通过利用分散元账框架，可应用在 oracle 区间存在的多种多样的工程结合到分散元账。因此最容易结合到现在在数据库上应用的工程 DB，MySQL，数据库管理系统等等上。在分散元账中可包含多种多样的信息，于是不但是应用原有智能合同的方法，而且在区块链元账账薄里可含更多的信息。MX 区块链分散账簿是经过下列过程来启动，且含许多信息来实行智能合同。

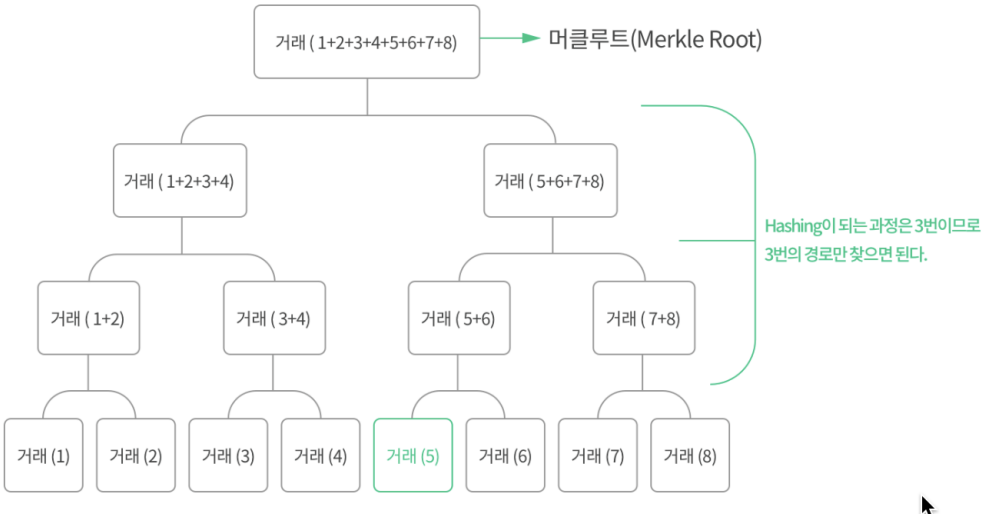


1 - 3 合同款式

Factor 区块链的合同款式是应用了原有的以太坊所具有的合同款式上的 oracle 区间 node.js, java, go ，使用了形成合同的方式。但是 factor 区块链的智能合同款式比这些支持更多的东西。 支持 Node.js, JAVA, go, C++, Python 等工程，即将会支持更多的工程。举一个最好的例子，若在金融司(Visa, Paypal, Mastercard, HSBC, CITI, America Express)应用这些来打造 oracle 区间，把这些连接到原有区块链来使用的方式。但智能合同是不可连接与下线链条信息及 API 等主要外部资源数据。因此原有的方式是经过多种多样的服务器来启动。但这些引起降低速度，服务器出错，关于互换性的许多问题，于是使用原有区块链在效率性方面存在着许多问题。但 Factor 区块链不是只依赖 middleware，而是以 Factor 区块链自体的性能，能够与原有工程进行互换。

1 - 4 Merkletree 储存款式

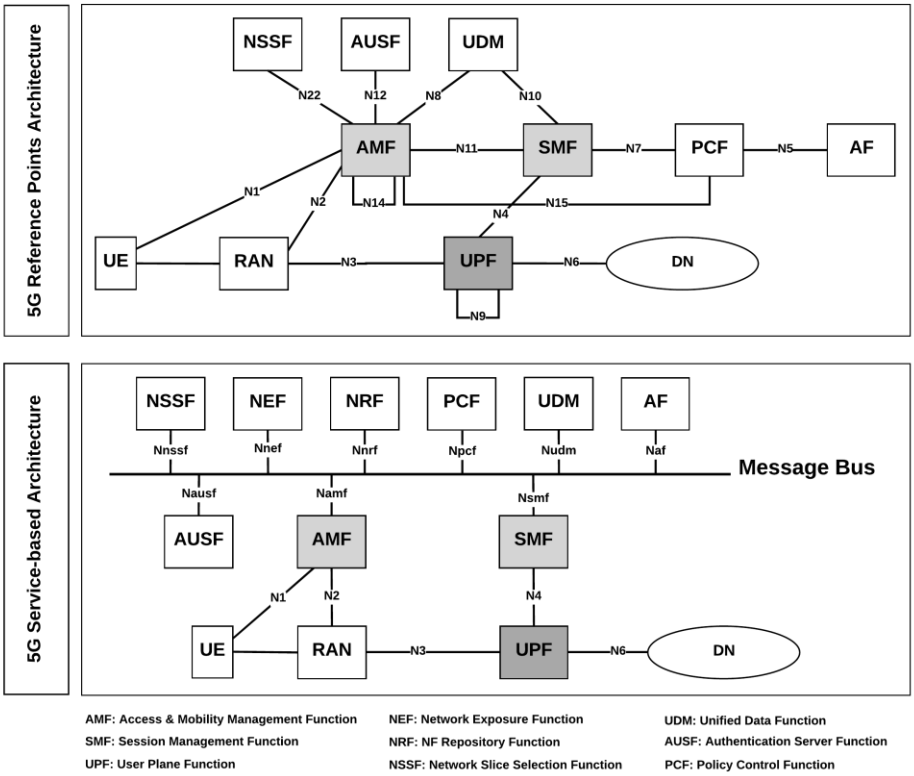
Factor 的 Merkle tree 储存款式是在原有的 merkle tree 授受二进数的值，于是也被称为二进 TREE。先参考一下下图。



在上图中的交易(1+2+3+4+5+6+7+8)值中，若要找交易（5）值的话，需要通过上图过程要找出值，才能找出信息的伪造真伪值，若交易量猛烈增加也能简单寻找特定交易。 SHA-256 方式是通过一个散列值，把从一个散列值中所出来的相互作用需要结合成 32bit，但在 factor 区块链 merkle tree 上的各个散列值经过连接和排列过程来形成。这就是说在原有方式上是支持 SHA-256 所拥有的一个散列功能(Funtion)， Factor 区块链提供着更多种多样的散列功能。而且在 merkle tree 上的验证过程中也不单纯是寻找特定交易径路，也能够找到各个区块拥有的固有号码(Nonce)值，时间戳 (TimeStamp)等等。 添加使用这些功能，能够提供更优秀的功能。

1 - 5 节点系统

Factor 的节点系统是使用添加 POS Masternode 功能的 node 技术。。这是脱出依赖在从原有的以采掘方式来形成的散列算力的方式。 也就是说，启动可使用 POW, POS 各个优点的协议。Factor 的 Masternode consensus 是修行提高网络连接维持性，保安性，速度的作用。这意味着结合 Factor 的专利 MX 节点的 spread 方式， Seed Node Technology 功能， 若原有的 Masternode 单纯使用在网络的维持性方面的话，Factor 的 Node 是与 Masternode 不需要形成那些功能， 也能够依据基本 Node 维持网络连接的 consensus 。下列是 5g 网络所拥有的 core 参考构造图。



上图是次时代的 5Generation Network, 也就是说是 第 5 时代的网络构造。（省略说明 5G 网络怎么被启动）在适用以上内容的智能手机上，若使用适用 Factor 协议的应用软件时， Node 不需要形成 Masternode，在具有更快速度的节点上继续加速，也就是说会带来速度逐渐加快的结果。这将会克服原有的节点增加，速度变得缓慢等现象，且会适应现在和未来的网络环境。因这些技术能够减少为了网络构造环境来使用的费用。

1 - 6 CORE 协议

Factor 的 CORE 协议是用 C 语言写成，且支持 window，Linux，Mac，raspberrypie（即将支持），Android, IOS 等等。 这是支持在 Factor 的 Core 协议中所具有的的多重 build 系统，同时支持多重语言。Factor 的 Core 协议是通过稍微复杂的过程来形成。

1 - 7 用户权限管理协议

MX 区块链是分为公开性分散账簿，闭锁性分散账簿。闭锁性分散账簿是利用在企业使用的形式，当形成区块链应用技术时为了解决保安问题。 闭锁性分散账簿是按照用户权限管理设定，能够接近公开性分散账簿。 此目的是应用这些，多种多样的企业，国家，集团，个人能够适合自己的用途来使用。

1 - 8 分散信息交换协议

Factor 的交换协议是信息要请人，提供人，代理人，拥有人都能够各个分散实行自己的工作。也就是说，Factor 区块链是具有这些信息权限的人能够安全，快速，容易使用服务。

1 - 9 应用软件 FRAME WORK

为了使用 Dapp(Decentralized application)的用户，在 Factor 中存在 Dapp Toolkit 和 One click Dapp。这是在一般 PC 进行开发时，防止因 Solidity 语言的编译和版本不一致而导致出错的现象，因此能够减少继续删除，修整，变更编译和语言等的麻烦。 而且,不但支持 Ether Solidity 语言，而且通过 Qtum, eos, neo 等等一个 toolkit 支持在多种多样的平台上存在的语言。 使用 One click Dap 可以容易添加，修整，变更需要使用的功能。因此这样形成的 Dapp 是在 Factor 区块链内连接的同时，在其它平台试图连接时，在各个不同的区块链平台上支持相同语言及可互换的网络，于是能够解决原有的其它平台所具有的费用，速度，互换，扩张等问题， 最终是个能够连接所有区块链的基础，也是个新的区块链统合型应用软件 Frame work。

1 - 10 内容管理模块

应用区块链分散账簿，可互换及连接许多技术。但需要管理，控制在区块链分散账簿上所含的信息，技术，记录，认证系统，医学系统等等的模块。例如，假设在区块链分散账簿包含医学信息，想把这个联动与 MRI。MRI 机器寻找人体的信息，把这些形成为一个信息传送到电脑，通过此信息用户判断此信息中含有什么内容，但若把人体信息包含到区块链分散账簿上的话，不单纯是判断含着什么内容，而且实时比较其它医学信息，且在医学手术装备上联动 MRI 上的信息，出来 MRI 结果，医学手术装备就能立刻进行手术。而且 DNA，认证身份，分析多种多样疾病等不需要花高费用。Factor 区块链是基于以上实际生活上的使用性来应用。

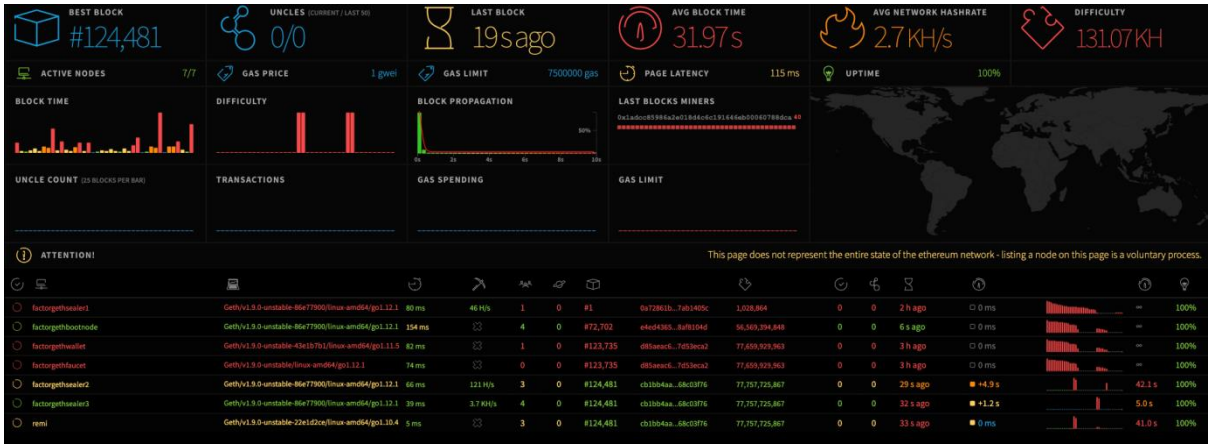
1 - 11 数据库

以前数据库的通用意义是用户收集信息，集合这些信息的叫做数据库。应用这些形成了现在的谷歌，NAVER,YAHOO 等通过这些我们能够提高我们生活水平。
但是在探索引擎上存在的许多信息按照用户的判断来改变信息的量，质量，正确性，也存在着许多问题。因此通过应用区块链的协议算法，正确选拔信息且解决所有问题点，再加上人工智能 AI 能够利用这些信息。 Factor 区块链是超越上述数据库的概念和规格，应用区块链用户的所有信息，同时在形成及使用信息上能够一起使用原有工程 （DB, Mysql, MSsql)。

2 连接性

2 - 1 Ethereum 连接性

现在以太坊添加 side 区块链，等离子网络，RDN，试图获取扩张性，且通过 sharding 加快速度，正在试图着通过这些解决多种多样的问题。但在速度及扩张性方面还是存在着许多不足的部分。但是用 Factor MX 区块链的 Dapp 按照下图链接时，Factor 拥有的技术力是联动与在散列中所含有的 26 个以上的散列，支持多种多样的开发语言，不但是增大原有的 oracle 区间的可支持工程的范围，而且速度也加快了。现存的使用以太坊的许多硬币也能连接到 Factor 区块链的 DAPP 上。尤其以太坊是随着节点数的增加速度就逐渐降低，但通过 Factor 区块链的专利 MX 节点 spread 喷射方式技术，随着节点数增加速度也逐渐加快。



2 - 2 Eos 连接性

原有的 EOS 是选定 21 个 BP，对此维持全体网络速度，当制作 DAPP 时存在叫做 RAM 的电脑资源性硬币。

若用 Factor 区块链的 Dapp 来连接 EOS 模块的话，在运营 21 个 BP 的过程中所需要的高费用，因 Factor 区块链的 Dapp，连接时增进速度和效率，能够从运营 21 个 BP 的高费用低效率方式变换为低费用，高效率方式。

而且在散列的连接性方面，当智能合同的功能连接到 oracle 区间使用时支持多种多样的 Solidity 语言，是与 Factor 的模块一样使用 Solidity 语言版本的区块链相互互换，以这样的方式使用 Eos 的许多硬币也可以连接到 Factor 区块链的 DAPP 上，能够发挥与 Factor 区块链一样的效力。

2 - 3 Neo 连接性

在 Neo 进行 Trinity ICO 中，直到 Neo 区块链达到 1816381~1816382 消费了 25 分。这是在 DBFT 的协议算法上超过(n-1)/3 个的节点引起伪造问题，在传送交易的节点上产生过负荷现象，于是发生了以上问题。若在 Factor MX 区块链用 Dapp 连接 Neo 的话，能够补完上述的协议算法的不足部分，而且依据专利 MX 节点提高各节点间的传送速度及连接性，解决 DBFT 协议算法问题的同时，通过 Neo 的 solidity smart contract 功能可支持在 oracle 区间存在的许多工程，于是能够修行克服 NEO 缺点的作用。

2 - 4 连接性的意义

MX 区块链是能够把原有的所有硬币连接到 Factor Dapp，相互连接各个分离的区块链的应用技术性，可使用许多功能，不但可使用在 IOT，无人汽车，人工智能等第四次产业，而且减少费用，通过卓越的扩张性会助于产业化。通过以上结果技术部主张成功实行区块统合链接。

3. 速度

3 - 1 速度性散列

含有 GPU，CPU 散列 Funtion 功能。

FACTOR 的速度性散列分为 A,B,C。这是可使用在 apple，window，renux 上使用的 32bit，64bit 相互不同的体系，且支持 GPU，CPU 多重处理功能。

散列 A

具有 1024 bit 状态，在 512 bit 输入区块中启动。 输入区块处理是构成为下面 3 个阶段

- 把输入区块状态的一半为 XOR
- 在适当状态上适用没有 42round 键的顺列（密码化功能）。这构成为下列 42 反复。
- 把输入分割为 256 个 4 bit 区块，在两个 4bitS-box 中通过一个各个连接。选择是以 256bit round 键来实现。把各个输入区块与键 bit 结合，通过 5 → 4 bit S- box 结合此结果。
- 关于 GF (2 4)使用最大距离分离代码，混合最接近的 4bit 区块
- 在下个 ROUND 为了能够接近相互不同的区块，指定 4bit 区块。
- 把输出情况状态为 XOR

结果文摘在 1024 bit 最终值，是第一个 224, 256, 384 或 512 bit。

SSE2 命令使用 set，适合与实现 bit 分割，每 bytes 提供 16.8 cycle 的速度。

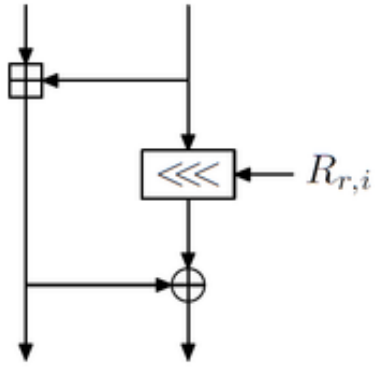
散列 B

B 散列的内部状态是输出大小的两倍且使用强烈的信息扩张，在压缩功能上使用被修正的前馈。这启动模式是安全与一般攻击。 B 散列的最重要构成要素是信息扩张，这设计为提供最少的距离。通过这些 B 散列防止解密。 B 散列是在压缩功能内部上具有并列处理特征，这是通过使用矢量命令可有效实现工作。 且可使用在许多体系结构 (x86 的 SSE ，PowerPC 的 Altivec ， ARM 的 IwMMXt)。

OS 模式 :	32 bit	64 bit
在 Core2 上 16 号散列速度		
16 号散列 256	12 cpb	11 cpb
16 号散列 512	13 cpb	12 cpb

散列 C

支持 256, 512 及 1024 bit 的内部状态大小和任意输出大小。在 Intel Core 2 Duo，对 64 bit 模式的输出大小要求每 bytes 别 6.1cycle 时，散列 C 的 Threefish 核心功能是以 MIX 函数为基础。MIX 函数是再次添加定数和 XOR，变换为两个 64bit 单词。 UBI 模式是结合输入链条值和任意长度输入文字列，形成固定大小输出。散列 C 的 Threefish 功能是 使用非线性加法和排他性逻辑的结合。这功能是最佳化在 64bit 工程，C 散列用途是随机散列，并列散列，个人设定等选择性功能。



3 - 2 Seed node

Seednode，也就是意味着种子节点，在用户使用 Client 模块时，最优先寻找节点，起着连接的作用。但是计算首先连接的 Seednode 速度慢，其它节点速度更快的话，不是首先连接到 seednode，而是连接到维持节点的网络后进行同步化。MX Seednode 技术是应用这些原理，计算全体节点的速度，按照速度顺次维持连接。这意味着随着 Factor 节点的添加，出现速度更快的节点的话，具有持续增加速度的效果，同时速度一般或添加较慢的节点的话，保留连接慢的节点，首先连接到速度快的节点，快速进行同步化
。添加速度慢的节点，也在速度方面上具有优秀性，不管速度，相互连接的节点逐渐增加，连接性逐渐提高。

3 - 3 Masternode

原有的 Masternode 是赋予网络维持性的话，收到硬币的补偿系统来起作用。 但 MX Masternode 比这些还具有着更多的功能。

① 提高交易速度
② 防御网络攻击
③ 帮助 Seednode 连接于 spread 方式
④ 可实行 Private Send
⑤ 监管(Governance) 功能
⑥ 低电力高效率网络赋予功能

3 - 4 MX node

基于 MX node 的 Consensus，在形成及运营 POS, Masternode POS 上具有下列规则性。

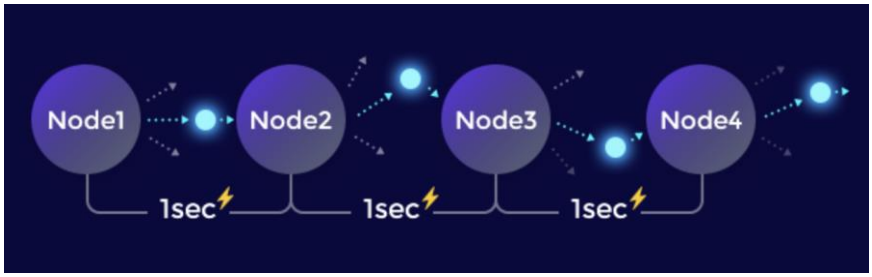
① GPU - 包含 CPU，支持 GPU 多重加速方式， POW 可支持的算力加速方式是支持 Factor 的 spread 喷射方式的加速方式。
② Seednode-像下列图[1]一样，
以喷射方式喷射的图[2]中，节点连接时招来连接目录进行同步化时使用自动连接的系统，与 Masternode, Normalnode, POW 比较速度，按照速度优先顺位来连接。因此在连接性方面速度非常卓越。

③ Masternode - 像下列 [图 1]一样以喷射方式喷射的图[2]中，当节点连接时 MX masternode 是具有连接维持性，于是同步化时能够加快连接速度。

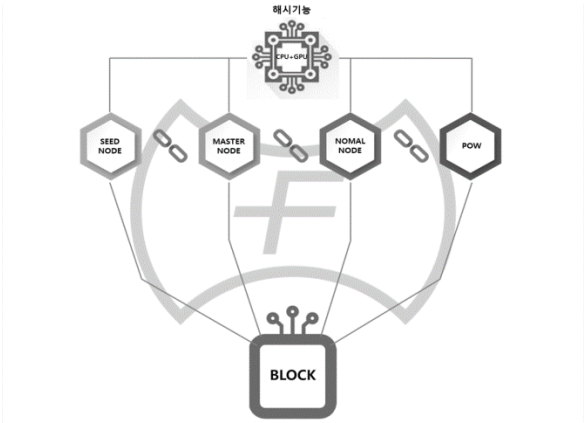
④ POW - 以像下列 [图 1]一样的喷射方式喷射的图[2]中，实行 Pow 的节点是在连接时助于加速化。 这是按照算力提高交易速度，随着速度快的节点添加，速度就逐渐加快。

⑤ Normalnode - 像下列 [图 1]一样以喷射方式喷射的图[2]中 ，当一般用户形成节点时若具有较快的速度性时，网络同步化时能够提高速度。

图 [1] SPREAD 喷射方式



图[2] MX Node system



详细说明 [SPREAD 喷射方式]

在图[1]一样的喷射方式上，像图[2] 一样存在 Seednode, Masternode, Normalnode, Pow 这 4 种节点。 图[2]的 4 种节点像图 [1]一样同时喷射，且选择最快的节点。首先，使用节点所具有的 MX 区块链的低电力 GPU 加速方式，在 Factor 的 Node 系统的速度方面上起着促进同步化，加速化的作用。 Seednode 的功能是同步化时带来特定节点目录，修行自动连接的作用，seednode 连接的同时通过所有节点的速度计算方式，按照速度优先顺位选择连接节点。以这样的方式连接后 Masternode 是通过节点间的连接性维持功能， 以速度优先顺位连接时巩固所有节点间的连接性，最终 POW 成为加速的方式，在所有节点上与速度快的节点连接。因此 Factor 的 MX 节点是每当添加节点时， 与速度快的添加节点数成正比，具有加速的特征。这是当节点数增加时，运营低费用高效率方式的 MXnode。.

3 - 5 Bootstrap

能提前下载原有的分散账簿。Bootstrap 是压缩之前存在的区块链信息，能够省略招来区块链信息的过程，能够减少同步化(Synronizing) 时间。 MX Bootstrap 技术是利用 MX 区块链提供的 SHA-256 函数，能够查看文件的伪造真伪与否。

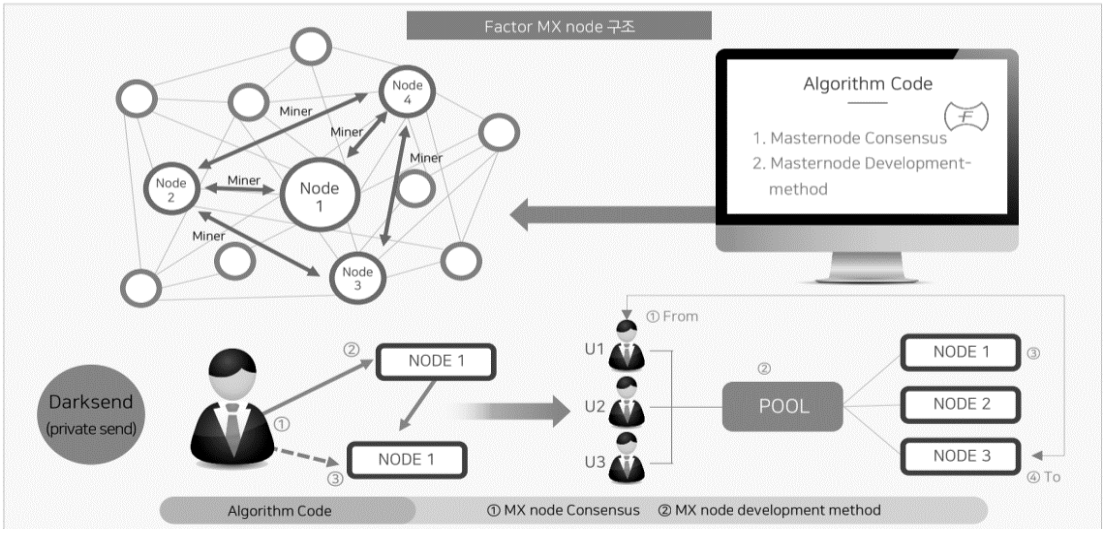
4. 保安性或安全性

4 - 1 Secp256R1 key

现在所使用的区块链的 Secp256k1 键方式为属于 ECC(Elliptic Curve Cryptography, 椭圆曲线密码技术) 方式的 ECDSA(Elliptic Curve Digital Signature Algorithm) 密码算法。在原有系统中作为 ECDSA 的 parameter 使用 secp256k1 curve， secp256k1 curve 是使用为为了制作 elliptic curve 的定数集合之一。 也就是说, ECDSA 是指密码化方式， secp256k1 键是在这需要密码化的数中将要代入的定数集合。 因此这样的 RSA 密码技术是在实际生活中使用为形成 WIFI 密码， ECC in JavaScript, window 运营体系 Cd-key, SSH-key 等等。但在这里问题点就是，若出现 量子计算机的话，因能够预测密码键值，进行复制的量子计算机的连算能力，于是 ECC, RSA 密码方式不能适用在未来。因此 MX 区块链是使用更安全的 secp256r1 方式，使用对量子计算机连算能力的保护散列。

4 - 2 Private Send

private send 功能的原理很简单。通过许多人发送交易，于是发送人不分明，具有提前保障匿名性的功能。 用户为了进行交易,将汇款金额输入到钱包,按 private send 键的话,您的钱包会将输入金额分为小单位金额。(单位:0.01,0.1,1, 10) 然后,用户的钱包会发送给具备网络上特殊环境设定的节点(Master Nord)。 每个 Masternode 在将用户输入的信息混合后,在 Masternode 用户的钱包中传送内容,并将分隔的汇款金额寄给自己,地址是以随机形式形成,发送到形成的地址中。 为了让你的资金完全无法追踪,你的钱包会重复这些过程,比如金额可以分割的任意数量,这样的过程一次结束,叫做"round"。 因此,经过尽可能多的 round 数量后,形成交易。 此外,mixing 过程在用户看不见的地方进行,在任何情况下,接收到的 Masternode 都不会接收个人信息。 因此, mixing 的 masternode 不可追击。



4 - 3 Merkle Tree 应用保安

在上述的 Factor 的 merkle tree 构造上，结合之前区块+ 现在的 merkle tree+ Time Stamp, Nonce 值形成构成 Blockheader 的一个区块。在这里应用 MX Block 的 Block Time Stamp, Nonce 值，在 merkle tree 构造的伪造检查方式上适用更卓越的保安方式。时间戳具有着把现在的时间值变换为 UNIX 值来进行记录的功能。在这里时间戳不单纯是记录区块的时间，而且引入 Factor 的固有区块。因此具有着检查伪造区块的功能，通过所指定的 Nonce 值的变换，在 merkletree 构造中检查适当信息时可缩短时间。因此 MX 区块链不单纯是依赖原有的 merkle tree 构造，而且减少了区块伪造检查时间，且提高保安性。

4 - 4 masternode 网络攻击保安

对 DDOS 攻击, 网络通信量攻击等等的网络攻击问题，通过依据 masternode 的网络维持提供优秀的保安水平。Masternode 是通过通信量分散系统，通信量拒绝系统，监管系统，当在一个节点上攻击较多特定攻击人的通信量时，其它节点可正常实行节点，若攻击全部节点也可以通过 masternode 的防火墙，连接特定端口, DNS 通信量防止攻击，较高的通信量收容力，监管系统可快速对应以上问题。

4 - 5 Oracle 区间保安性

把区块链外部的环境命名为 orakle 区间。这是指在 orakle 区间存在的工程连接到区块链上，在实质性外部环境中启动在区块链中所实行，命令的东西。当在 orakle 区间存在的 JAVA, NodeJS, Mongodb, Mysql 等工程连接时，在 Factor 区块链内检查保安性，启动性后实行工程。因此当许多工程与 MX 区块链连接时，通过各工程间过滤过程进行连接。但向后关于 MXblock 联动时确认安全性的工程是即将在 Dapp Toolkit 公式支持。

4 - 6 保安性散列

FACTOR 区块链的保安性散列 D,E 是起着下列保安性散列功能。

- 散列 D

对 SHA-3 的 D 散列-f [1600] 区块变换 f 是使用 XOR , AND 及 NOT 连算的排列，且能够在软件及硬件上容易实现。这是定义 2 的 word 大小 , w = 2 ℓ bit。主要 SHA-3 是使用 64 bit 单词, ℓ = 6。

排列 5 × 5 × w bit。使用主要 indexing 来假设 $a[i][j][k]$ 是输入的 bit $(5i + j) \times w + k$ ，也就是说*前 选择 J* 列, 还有 *k 是指 bit。*

Index 算术是第一二次元修行为 5 模块，第三次元是修行为 w 模块。

基本区块交替功能是构成为 $12 + 2\ell$ 的 5 个阶段。

对量子攻击的保安

一般计算机(Grover 算法)可以进行量子计算机 √ $2^d = 2^{d/2}$ 结构化的自由图像攻击, 而古典的 brute-force 攻击则需要 2^d 。 结构化自由图像攻击意味着第二次自由图像攻击和冲突攻击。 量子计算机还根据特定指定日期进行攻击,破坏碰撞耐性, ^{3} √ $2^D = 2^{D/3}$ . . 若最大强度为 c / 2 时对 SHA-3 的量子保安提供下列上位界限:

例如	Bit 单位的保安强度			
	冲突 (Brassard et al.)	冲突	自由图像	第二个图像
SHA3-224 (*M*)	74/3/3	112	112	112
SHA3-256 (*M*)	85 1/3	128	128	128
SHA3-384 (*M*)	128	192	192	192
SHA3-512 (*M*)	170/3/3	256	256	256
SHAKE128 (*M* , *d*)	分 (*d* / 3,128)	分 (*d* / 2,128)	≥min (*d* / 2,128)	分(*d* / 2,128)
SHAKE256 (*M* , *d*)	分 (*d* / 3,256)	分 (*d* / 2,256)	≥min (*d* / 2,256)	分 (*d* / 2,256)

- 散列 E

不仅是 E 散列-128,原来的 E 散列是 128bit 结果太小,且因设计上的弱点导致安全问题,因此被视为不安全。 256 及 320 Bit 版本的 E 散列是分别提供与 E14 散列-128 及 E 散列-160 同等水平的保安。 安全水平足够,但设计为需要更长的散列结果的应用程序用。
E 散列-160(RIPE 信息)是一般以 40 位数的 16 实数来表示。 下面显示 43Bytes ASCII 输入及相应 E 散列-160 散列。

```
E 散列-160("The quick brown fox jumps over the lazy dog") =
 37f332f68db77bd9d7edd4969571ad671cf9dd3b
```

E 散列-160 是与密码化散列函数（小变更，例如把 d 变更为 c 的话成为完全不同的散列）的 everlanch 效果一起启动。

```
E 散列-160("The quick brown fox jumps over the lazy cog") =
132072df690933835eb8b6ad0b77e7b6f14acad7
```

长度为0的文字列的散列值如下。

```
E散列-160("") =
 9c1185a5c5e9fc54612808977ee8f548b2258d31
```

5. 扩张性

5 - 1 Factor ledger Module

Factor ledger Module 提供多种多样的功能。现在可提供的主要功能有追踪动物，债权，汽车竞买，数码财产，基金开设，贸易交易信用证，游戏，管理食品，认证身份，交易所，汽车生活周期管理，汽车整备周期管理等等在现实生活中具有着多种多样的用途。 Factor ledger Module 是通过应用区块链技术减少费用，具有卓越的技术力，且提供多种多样的 BA 网络，而且以低费用可以发挥出高效率效果。应用这些可适用在原有工程。

5 - 2 Graphene

Factor Graphene 模块提供稳定价格密码货币,分散化资产的交换,在产业要求的性能和扩展性,可操作性账户的许可,账户的招募和可计划的支付,补偿程序,用户资产，可变换的账户，DPOS协议一致等服务。在 UIA 系统中,可将无形资产嫁接到 Token 上使用,并可按类别分享资产。此外,如果想把在企业使用的区块为非公开的形式来使用,则通过主动性账户许可功能获得认可的用户可以使用,并适当形成多种商业模式(BA)。Graphene 模块是利用上述功能， 使公司能在实际生活中发挥的纯功能,运营和管理等。 因此,对于解决现有区块链难以作为企业运营的问题,意义重大。

5 - 3 金融

Swift 系统的分散账簿
IBM Mainframe (统合银行电算系统)
HP UNIX (次时代系统)
HP Superdome (统合次时代系统)
IBM UNIX (WINS)
把在第 1 金融，第 2 金融，第 3 金融等金融圈上使用的 swift 系统，在正使用中的金融圈系统规格上使用 Factor Dapp 和 Toolkit 活用在金融圈。

5 - 4 IOT

AMQP(Advanced Message Queuing Protocol)
CoAP(Constrained Application Protocol)
DDS(Data Distribution Service)

JSON-LD(JavaScript Object Notation for Linked Data)
MQ Telemetry Transport
Near-field Communication
Supervisory Control and Data Acquisition
6LoWPAN, HomeKit, IoTivity, LoRaWAN, Zigbee

5 - 5 公共机关

对于信访文件,国民投票,身份证明确认用信访登记文件等,Factor 区块链将起到节省大量费用,提高安全性。

5 - 6 物流，流通

CRM, SCM, ERP, Logistic System
在产品间的物流移动中可查询 QR 码，在流通系统中作为分散化的账簿，可确认部分内容也可以查询。

5 - 7 制造，生产

区块链是最先适用于在制造和生产中使用的机器人。 这意味着把机器人所具有的语言修行功能应用到区块链分散账簿运行。

6.Dapp(生态系)

6 - 1 Factor Dapp

① 概括及生态系概要
② 技术生态系
③ 监管生态系
④ 应用软件生态系
⑤ 运营方式及参与方法

6 - 2 Factor ToolKit

支持 Factoremix 和 Oneclick Dapp。Factoremix 是在开发部分上支持使用在 FACTOR Ethereuem, Neo, Eos 模块的语言。 而且通过使用 Oneclick Dapp，当 Dapp 用户按键的话就形成 Dapp, 在构造 Dapp 时具有卓越的便利性。向后在 orakle 区间会添加可互换与区块链的多种多样工程将添加到 Factor Toolkit 上，不但是 Dapp 开发人而且一般用户也能连接区块链进行应用开发。

6 - 3 支持语言及工程(orakle 区间)

① Go 语言

由谷歌开发,是目前与区块链连接时使用的元素之一,语言的设计和 Go 的语法大体上类似与 C 。代码模块围绕中括号,具有着包括 for,switch,if 等的一般控制结构。 与 C 不同,分号不是必需而是选项。 变数宣言是不同写作的选项。 明确变换型号,为操作并行性程序使用 go 和 select 关键词。 新类型是有 map,Unicode 文字列,排列 slice,还有为了内部通信的渠道

(channel),Go 在不太理想的硬件上也能快速进行编译。 Go 是成为 Gavizie 系列的语言,与并行性(concurrency)相关的 Go 的结构性规则(从 channel 和选择性 channel input)是从 Tony Hoare 的 CSP 中带来的。 在 C++, JAVA 的功能中,类型继承, Generic,启明(assertion),Messard Overloding,Pointer 运算不包含在 Go 中。 因此,作为 Go 语言的开发语言,可将不足的部分用其他可支持的 Oracle 区间语言加以补充。

② JAVA

是客体指向程序设计(Object-Oriented Programming, OOP),指向程序设计是使用为把握“客体”单位。 每个客体都具有传递信息,数据,便于变更程序的功能。 因此主要用于大规模软件开发,开发维护,维修简便。 可进行直观性代码分析，但过分的客体化倾向是在实际开发时不可适用许多开发要素。在 Java 上 javac.exe 工程起着编译作用,Java 是在 JAVA 实行环境（JRE:java Runtime Environment）上安装的所有操作系统中可以实行。 从 JAVA version 8 开始支持 Lambda Expressions,过滤,操作,统计处理操作容易,支持简练代码函数工程。C++为了去除存在储器生成的客体,C 开发者必须亲自写作代码,但具有着自动去除不使用的客体等功能。由此可实现多种多样的应用软件，且可以容易实现多线程工作。

③ Node.js

立足于现有 Java 的问题性,使用着 V8 发动机。 这将会依据谷歌持续更新及添加功能,使用活动的 Driven 方式。 这是在用户发生活动时，用输入装置传送数据时才能启动的方式。 仅针对发生的活动,网页服务器提供"连接",因此可以最少化资源,大部分网页服务器在用户发生活动之前一直运行,因此等待时间,存储器消费量会增加。 并且使用 Non-blocking I/O 方式,现有方式一旦发生 Read/Write 活动,将立即独占所有相应模块,中断用户程序的所有工作,并在相应活动中使用所有存储器， 但 Non-blocking I/O 是一旦开始活动 ，就变换模块能够准备其它工作。 因此,速度会比现有的同步式更快,而且也少占存储器容量。且具有客户端和服务器语言相同的优点。

④ C, C++语言

C 这个语言非常简单,从软件构成的最小单位 bit 开始,到存储器管理,可使用高级概念 OOP。实际上,最底端的 OS API, 几乎都是 C 语言,此外大部分基础设施软件都是制造为 C 之后提供其他语言条形码。 从低端开始提高层次进行观察,机器代码会随着机器的不同而变化,而 Assembly 也根据 Intel/AT&T 等语法存在几个版本,但在上面还是统合为 C 语言。而且 C 语言再往上去，会再次分为 C++/ Java/ C#/ Objective-C / Python 等多样的语言形态。 因此,实际上不使用 C 语言，使用其他高级语言,也可以联动使用， 在这种情况下,有无数的语言和 C 语言提供的 FFI 事例。

7. 游戏

7 - 1 INREAL 引擎
7 - 2 UNITY 引擎
7 - 3 下腹引擎
7 - 4 CRY 引擎
7 - 5 丘比特引擎

7 - 6 游戏 BRIO 引擎
7 - 7 探索引擎

8 保安方案

8 - 1 Factor 疫苗
8 - 2 Factor Online Security
8 - 3 Factor 企业型方案

9. 用语

MX(Multi X)区块链

MX 分散元账

ECDSA(Elliptic Curve Digital Signature Algorithm)
是属于 ECC(Elliptic Curve Cryptography) 方式的，使用为数码签名用途的密码算法。 ECC 是作为 RSA 密码方式的对案在 1985 年提案的方式。若密码键的长度长的话，就强化保安，因密码连算速度减少，因此为了强化保安， 代替延长 RSA 方式的密码键长度，使用 ECC 方式。

secp256k1
是 ECDSA 的 parameter，使用 secp256k1 curve。secp256k1 curve 是指定为标准，是为了制造 elliptic curve 的定数集合。这叫做 “Elliptic curve 256-bit domain parameter” 。构成为 sec(Standard for Efficient Cryptography) + p(Parameter p over Fp) + 256(Field Size p 的 bit 数) + k(Koblitz curve 变形) + 1(sequence number) 。

Secp256r1
是 ECDSA 的 parameter 使用 secp256r1 random curve。像 secp256r1 一样, 代替 k 使用 r(Random Parameter)的 Curve。

MX 节点
MX 节点是维持网络连接，起着解决因少数采掘集中化现象而导致的问题点，这是通过采掘服务器和节点的相互作用，可形成更坚固更安全的分散型区块链。

Merkletree

Factor MX 区块是形成起着相互作用的散列 tree，即 Merkletree，当需要检证部分信息时，只知道此中一个节点值的话，就能查看关于此节点的所有信息。 而且形成的区块持续连接与之前区块，因此形成具有强烈保安性的区块链。

Hash(散列)
散列函数是指对具有任意长度的任意信息上用固定长度的信息来进行 mapping 的函数。适用这样的散列函数出来的固定长度值叫做散列值。这值也被称为散列代码，散列 sum，checksum 等。散列函数是构成为简单的算法，于是相对来说比较少消费 CPU，memory 等系统资源。而且对相同的输入值保障相同的输出值。也存在以特殊目的用途形成散列值的原本和收到另外的值对相同的输入具有不同输出值的散列函数。散列函数是不管输入不同，也存在输出相同值的情况。详细原理是使用鸽巢原理。这样的情况叫做‘冲突’。按原则散列函数是除了这些没有方法的冲突之外，不可有意计算冲突。按照这些特性，存在着许多用途的散列函数，且在下列部门上有效使用。

- 资料结构
- 散列 table
- 散列 set
- Bloom filter
- 硬币
- 查询重复 lecord
- 查询类似 lecord
- 查询类似部分文字列
- 几何散列
- 探知伪造/检出错误

近来出现的很多语言是在基本库中都含有散列函数,不需要实现,可立即提取散列值来使用。但有些老语言需要通过设置扩展库或直接体现的方式来解决。 以派森为例,为了在词典(Dictionary)中加入等级,必须要体现散列函数,同时还要体现散列的比较函数(cmp)。如未体现散列函数,则以散列值代替其客体的地址值。

作为有名的散列算法有 Message-Digest Algorithm(MD)和 Secure Hash Algorithm(SHA)等。各算法是因严重的散列冲突问题等, 改善散列函数,按发表的顺序,以 MDn,SHA-n 的方式进行跨越。但 SHA-2 是例外,SHA-256,SHA-512 一起被称为 SHA-2 族(SHA-2 family)。以 2014 年为准, 最新版本分别 为 MD6,SHA-3 或普通版本使用自己所用语言中提供的库里包含的基本散列函数。

ECC(椭圆曲线密码技术)

ECC 是"有限体(Finite Field)上的椭圆曲线(Elliptic Curve)"——用英文是利用" Elliptic Curve over Finite Field "的数学性性质的密码技术。 ECC 作为 RSA 密码方式的替代方案,是在 1985 年提出的方案。若密码键的长度(以 bit 数表示)长的话,虽然会强化保安(解读密码需要很多时间),但是因为加密速度变慢,为了强化保安,使用 RSA 方式。 即使用 ECC 的话,用较少的 bit 数的密码键表示相同的密码性能(解读密码上所需的时间)。 例如,3072-bit RSA 和 256-bit ECC 的密码性能相同。 bit 数少的话,运算处理得更快,所以密码运算性能更好。 从另一个角度来说,即使加密设备的 CPU 性能低,也能保持加密性能。

9. 结论

下列整理了在本技术书内容中所查看的FACTOR mx区块链的技术。

1)Factor mxblockchein采用主区块的secp256r1方式,开发并搭载了26个以上的新散列算法功能,此后如果出现新技术量子计算机的话，可追加更新。

2)Factor mxblockchain的技术不仅与现有的硬币连接,还可以互换。

3) Factor mx 区块链也是与比特币相同的采掘方式,虽然具有半衰期功能,但高的散列功能的电力消耗量却减少为比特币的100分之1左右。

4) 可以互换pow,pos功能,并设计成可以采掘master node,任何人都可以开采。

5) mx区块链的节点选择方式是获得专利的spread喷射系统,设计成优先顺位节点选择方式，比原有节点选择方式在速度方面更加卓越。

6)在区块链的分散账簿上装载量子力学保安功能，在Oracle区间也具有优秀的保安性。

7)mx 区块链是自体开发的主要区块链，有转换器(dapp)功能,因此可展现许多的扩展性。

8) mx区块链是利用转换器开发工具,不仅是新开发者,任何人都可以容易接近并使用。

9) FACTORmx区块链保有7种游戏，在这里用factor dapp连接了mx区块链。

10)FACTORmx区块链是与mx区块链和人工智能结合，能够活用在所有产业化系统，提高了生产性降低费用，为了打造安全产业社会，FACTOR研究部会为了开发不断做出努力。

< 试验信息及结果>

免责条款

在本技术说明书提出的内容仅以提供信息为目的,本文件不得依赖陈述。我们对不承担在本技术说明书明示的所有信息所发生的任何法律责任。尤其是在本说明书明示的‘开发技术’是会有所变更，而且与硬币性能及收益等没有任何关联。在本技术书上的信息是没有承认的规制机关。 因此,根据管制要求或管辖规则,不得接受任何必要的法律措施。 在本技术书的发行,分发或推广方面,准据法和限制条件也不受规则约束。 在技术书中的信息会加以变更。 Factor Flock 锁链不断研究,因此此后在"修改版本"部分上可确认变更事项。