CUBE
CHAIN

# Cube Chain

Technical White Paper

© 2018 CUBE CHAIN. All Rights Reserved.


# Contents



© 2018 CUBE CHAIN. All Rights Reserved.

# Cube Chain 技术白皮书

Cube Engine Version 2.0

## 1. 概要

### 1.1 概要

区块链是一个分布式数据存储系统，以时间为单位存储数据并生成区块，通过加密区块的哈希(Hash)值进行对数据的验证。即，通过加密化进行数据验证并对相同数据进行分布式存储，从而确保数据的可靠性和稳定性。与常用数据库相比，区块链的优点在于可按时间顺序对数据进行加密化验证且不可逆，并通过P2P方式将同样数据共享并存储，从而更加安全地保护及维护数据。随着区块链被数字货币技术所运用，得到诸多用户的信赖，成为今日加密货币市场的基础技术。虽然区块链使用加密化方式及P2P方式呈现了独特的数据存储方式，为新技术开辟视野，但仍存在技术局限性。如果区块链要想完全取代现有数据库，必须伴随现有数据库的技术功能，例如提高速度和易用性等。倘若，区块链技术持续发展直至可取代数据库，那么它将成为存储和管理数据最具安全的方式。基于此观点，Cube Chain通过“CUBE”新概念代替区块，将数据库技术元素的可扩展性予以构造化。为了能够安全地使用公共数据库，数据库几项优点的运用将基于现区块链的优点。Cube Chain的研发将在确保先进区块链的原创技术下，发行加密化货币，并推出需要公开数据库的各种在线服务。

### 1.2 基本信息

**Cube Chain (QUB)**

**币名称** : Cube Chain

**总发行量** : 120亿个

**算法** : SHA256、CH-S1、CHF、SHA384

**奖励方式** : POH (Proof of Hybrid: POW+POS)

**POS参与条件** : 钱包内最少持有5,000个以上Cube Chain

**开发初始** : 2017年 1月

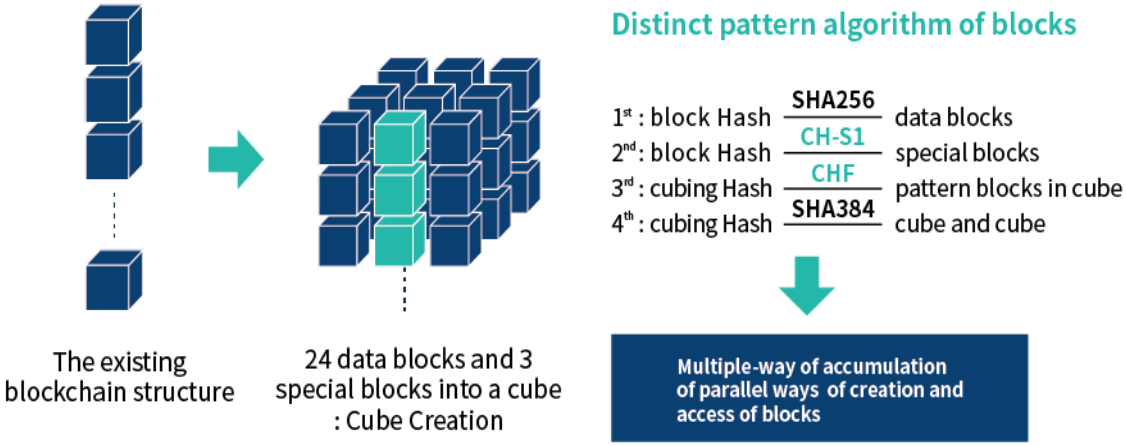
## 2. Cube Chain的特征

首先，对区块链的核心技术既加密化技术术语的哈希(Hash)进行如下说明。这是对SHA256的定义，是加密化哈希的一种。哈希是指“将特定数据转换为固定长度的数据”。在此，”。在此，象征的数据，若原有数据只要有一点变化，就产生完全不同的特点。其有助于保持完整性。例如“A”字符串的哈希与“B”字符串的哈希，仅因一个字母之差，其结果将千差万别。例如，典型的哈希加密算法SHA256，无论输入值如何，一般都将以256bit的其他64位16进制转换输出。


**[ 图 1 ]**

### 2.1 Cubing

Cubing是区块的集合体，将27个区块集成为一个Cube，即Cube化技术。记录交易账本的24个一般区块与3个特殊区块相结合，生成一个Cube。它不是一个简单的Grid概念，而是同时生成区块的并列技术。生成27个区块的同时，进行Cubing(CUBE化)，生成的CUBE又将产生一个新的哈希值。随后记录的账本将持续生成CUBE，哈希值将CUBE与CUBE进行连接，而并非是区块之间的相连。区块与区块相连形成首次加密化，CUBE与CUBE相连形成二次加密化。比现有区块链更加强大的加密技术，使生成区块的同时进行Cube化，生成的CUBE又将产生一个新的哈希值。通过Cubing产生CUBE的哈希值，并与区块的哈希值相结合，构建一个双重认证的数据系统。



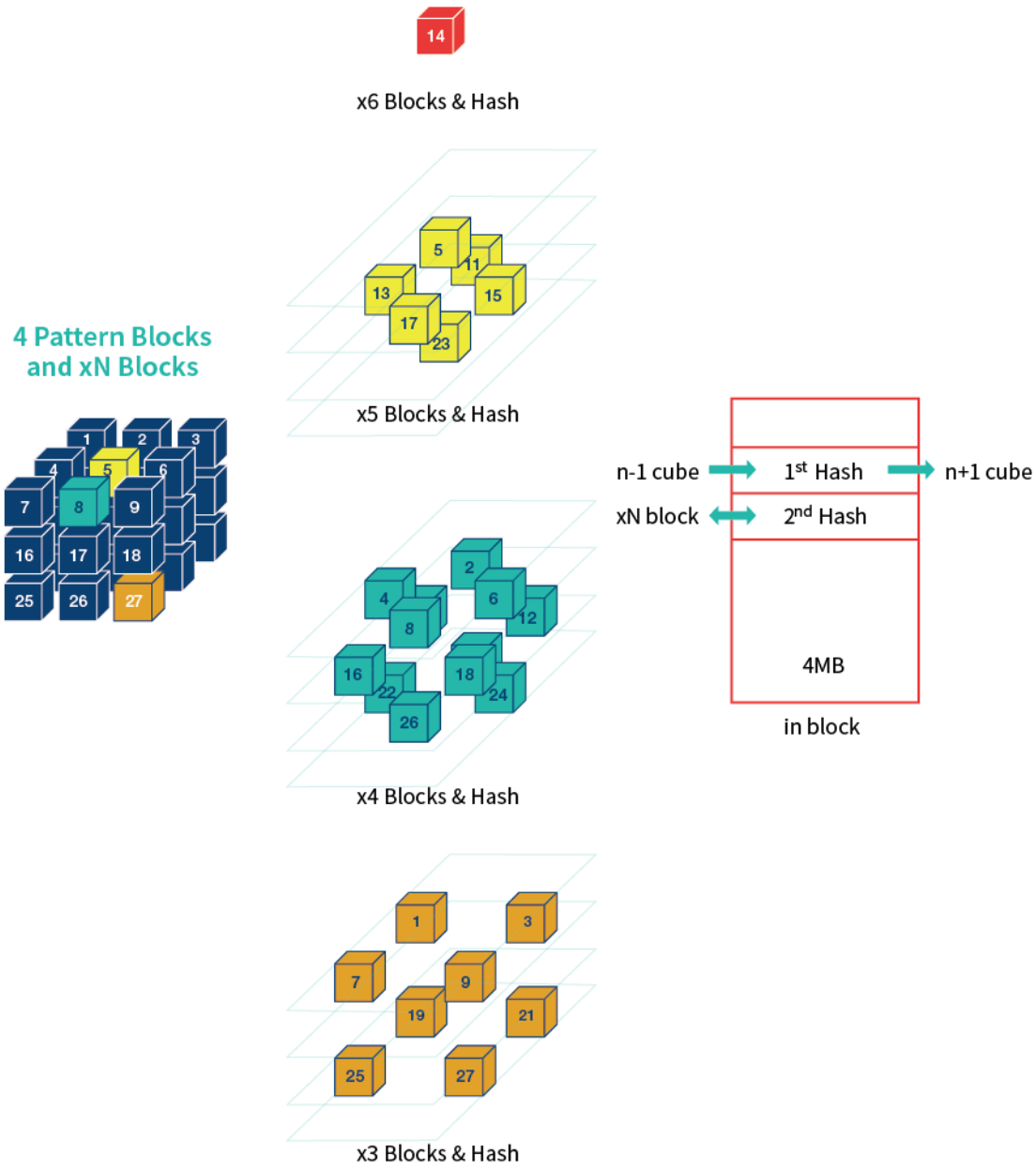

**[ 图 2 ]**

Cube Chain通过24个交易池及并列结构，快速又安全地生成数据区块，从而解决了因单链结构导致的速度迟缓和扩展性问题。在交易池中，同时生成24个数据区块直至加载到CUBE，其处理过程即快速又安全。此技术的设计旨在通过Cubing技术管理海量数据区块的并列处理，并通过双重哈希和模式区块结构实现区块间的快速访问。

区块合并成为一个CUBE，使用4个哈希函数强化了其安全性。此时，使用的哈希函数是SHA256、CH-S1、CHF、SHA384，其中SHA256和SHA384为公共哈希算法。下面讲述一下，自主研发的哈希算法：CH-S1(CubeHash Special Version 1)用于特殊区块的哈希函数；CHF(CubeHash Function)用于Cubing过程中模式区块的哈希函数。

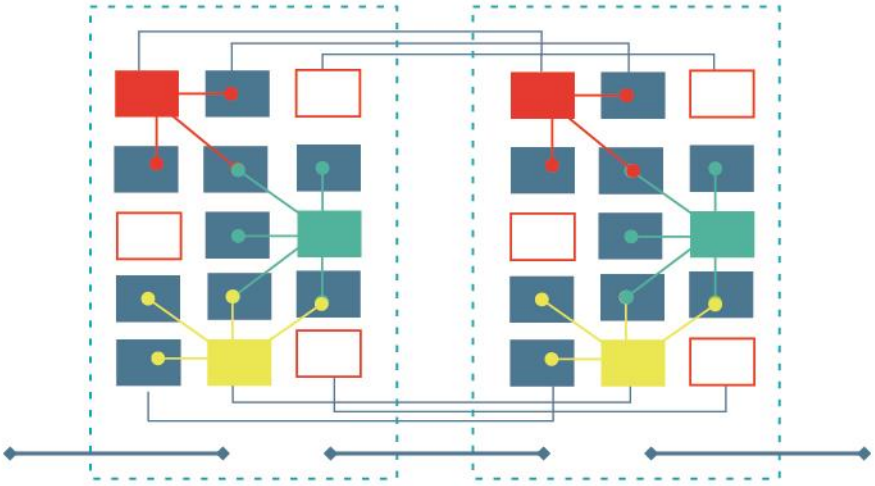
**结构分解与说明**

Cube Chain结构具备多重方式的区块装载、并列式区块生成及访问，有效提升了速度。


14
x6 Blocks & Hash
5
11
13
15
17
23
x5 Blocks & Hash
4 Pattern Blocks and xN Blocks
1
2
3
4
5
6
7
8
9
16
17
18
25
26
27
n-1 cube
1st Hash
n+1 cube
xN block
2nd Hash
4MB
in block
2
4
6
8
12
16
18
22
24
26
x4 Blocks & Hash
1
3
7
9
19
21
25
27
x3 Blocks & Hash

[ 图 3 ]

如图所示，CUBE分解将呈现4种区块模式。



**[ 图 4 ]**

每个模式区块将与前CUBE最临近的区块相连，[图2]的2nd Hash将存储xN区块的哈希值。
对于通过Cubing连接CUBE，因上一个CUBE哈希值存储于[图2]的1st Hash中，所以自然而然地将与上一个CUBE进行连接。由此形成区块与区块的连接，CUBE与CUBE的相连。通过各模式连接的区块哈希值将存储于CUBE内。

### 2.2 Indexing区块

Indexing区块是将所有区块的数据通过索引的方式进行有序编排，以供检索。Indexing区块是数据区块，它将所有交易信息的电子钱包以地址划分，并对各交易的CUBE高度(现区块链的区块高度)进行整理。因此，通过Indexing区块，可在短时间内更快地索引出相应的数据。

例如，A地址: CUBE区块位置20c(20为第20个CUBE; c为第3个区块), 32a, 105h, 201j, 302r 区块高度； B地址: CUBE区块位置 3b, 102v, 201s, 1001q 区块高度； C地址等: CUBE区块位置5c, 34e, 56g, 234k, 456y等，将地址以地址值进行依次有序排列，再根据地址值整理相应的区块高度。若要查询B地址内的指定交易，只需查看Indexing区块内B地址数据即可。Indexing区块旨在对指定地址进行整理，助于快速查找及便于管理。

**[现区块链方式]**

在搜索指定钱包地址的相关交易明细时，需查看所有数据。
(CUBE数为1,000个，CUBE生成时需查看24,000(1,000x24)个区块)
时间复杂度 = **O(B log2 T)**

**[Cube Chain方式]**

无需使用相应数据信息(钱包地址、CUBE高度、区块位置)来扫描整个区块，只需要在 Indexing区块内搜索钱包地址即可获取相应数据。
时间复杂度 = **O( log2 I + log2 T)**
例) 在搜索指定钱包地址的相关交易明细时，只需查看Indexing区块(1个区块+1个CUBE)

### 2.3 Statistics 区块

Statistics区块将对所有区块的统计值进行整理，在应用服务和各种API中呈现快速逻辑，并提供各种可用性。Statistics区块可确保数据的快速处理。例如，Statistics区块内将持有5,000个以上者为POS对象，因此可以对5,000个以上持有者的电子钱包地址、持有量多的电子钱包排名前1,000位、转账次数100次以上的电子钱包列表进行统计整理。此外，还可以对常用数据进行统计， 便于随时快速输出列表。

如果没有对这些区块的统计数据，索引必定会需要很长时间，但使用Statistics区块可以实现服务的快速处理。事先对持有量多的电子钱包排名前1,000位、转账次数100次以上的电子钱包列表等常用的输出数据进行统计整理，提供有效、快速的索引。其结果，可快速呈现相应应用服务的API。

例) 根据CUBE高度搜索POS对象，查看所需区块。

**[现区块链方式]**

CUBE高度为1,000时：1+2+3+ … +998+999+1,000=500,500x24=12,012,000个区块
CUBE高度为10,000时：1+2+3+ … +9,998+9,999+10,000=50,005,000x24=1,200,120,000个区块

**[Cube Chain方式]**

CUBE高度为1,000时：1+1+1+ … +1+1+1=1,000个区块
CUBE高度为10,000时：1+1+1+ … +1+1+1=10,000个区块

CUBE累计量达1,000个，所需查看的区块数量将相差10,000倍以上。如果，考虑到列表整理的过程和对相应明细的检索过程，其差异将更加显著。截至目前，考虑到的统计功能有：单笔交易1000QUB或2000QUB以上、持有量排名1~1000位、总交易量/总交易次数、未经授权的托管等。

### 2.4 Escrow区块

所谓Escrow是指中立的第三方仲裁 ，在交易中可增进买卖双方之间的信任，促进金钱或物品的交易。同时可确保交易的安全性。具体在卖方、买方、第三方之间进行，其过程如下:

买方将货款让第三方暂时托管，卖方从第三方得知入款的信息后，向卖方发货。买方收到货物后，确认货物与交易内容的一致性(如果交易货物不一致，可进行退货或取消交易)。买方对货物满意时，通知第三方收到货物。第三方将货款付给卖方，卖方确认货款，即交易成功。仲裁的第三方收取一定金额的手续费为一般Escrow的交易方式。

Cube Chain的Escrow交易中，尽管交易已签署，但接收方却无使用权，必须经过授权才能使用。 一般交易将存储于24个区块中进行分散而被记录，但Escrow交易数据则存储于Escrow区块中。
加密货币Escrow转账时，将向交易者双方发放认证密钥，双方可通过认证密钥进行授权。此时，将认证密钥，可分为自动随机生成的方式，由发送人发送的方式。密钥的授权方式多样化，可分为发送人认证、接收方认证、双方认证以及自动认证方式。自动认证是指对认证时间进行设置，认证将在指定时间自动完全，即接收方在指定时间以后将自动获取使用权。如果，发送人取消自动认证，认证方式将直接转换为普通认证，直至Escrow允许状态。这样，接收方无法取消交易，发送方也得不到使用权，从而形成一种相互约束，继续维持交易或合约。接收方的密钥认证方式为发送方通过电子邮件或Messenger等方式传递给接收方。现有的Escrow交易是由中介者在交易者之间充当交易的中介角色，Escrow区块特征为无中介者的Escrow功能。当然，根据实现不同的服务，也可以扮演原始方式的第三方中介角色，但其最大特征为将Escrow引用于当事者之间的直接交易中。无论是在线购物网、公开市场，还是个人之间的直接交易，Escrow都将成为一种即快捷又安全的交易方式。

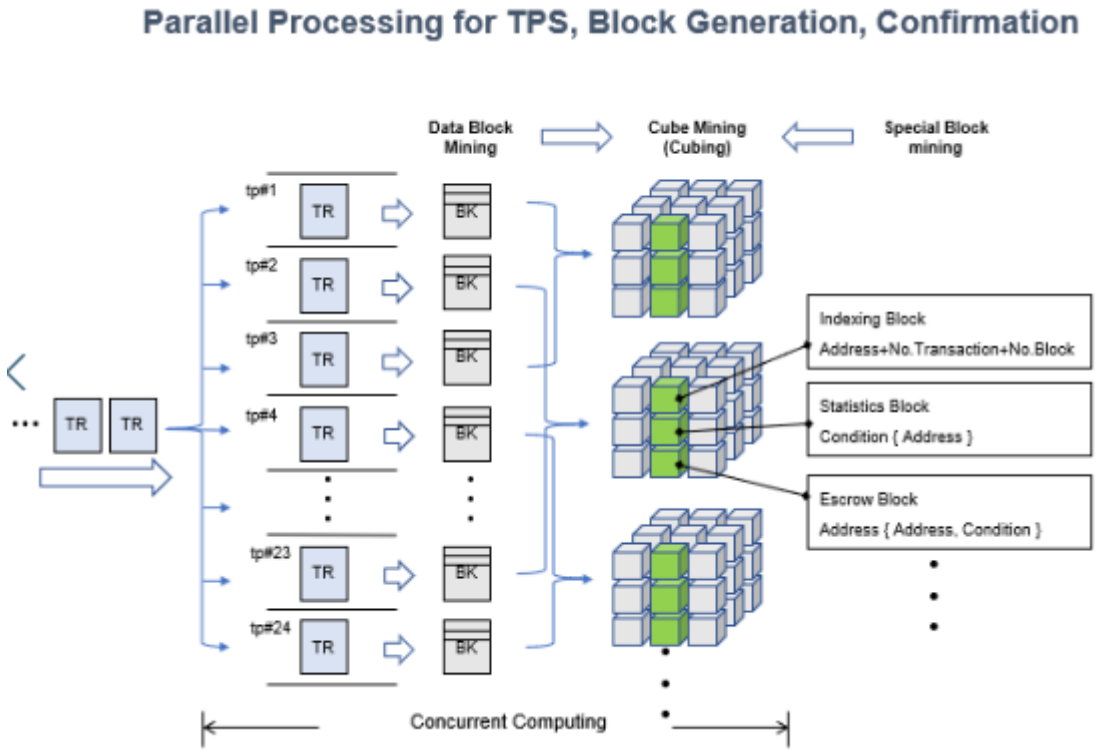
Escrow区块导入双重认证方式(Double authorization data system)来存储数据。一般数据将存储于24个区块中的任意一个区块中，但Escrow数据将被独立保管。Escrow数据在完成双重认证的同时将转为一般数据重新记载。双重认证方式是指在一般区块链交易时，除电子签名以外，将额外追加发放认证密钥，只有完成认证才可进行交易。
采用Escrow区块的此方式在加密货币中，尽管交易已签署，但接收方却无使用权。并非第三方中介的Escrow状态，而是赋予一种功能，来保护交易双方之间的交易。这是基于区块链的Escrow功能。
另外，Escrow区块还可当作密钥来保护数据。数据并非公开使用，只有通过加密化获取密钥者才有权验证数据。

**一般区块和特殊区块的大小及生成所需时间**

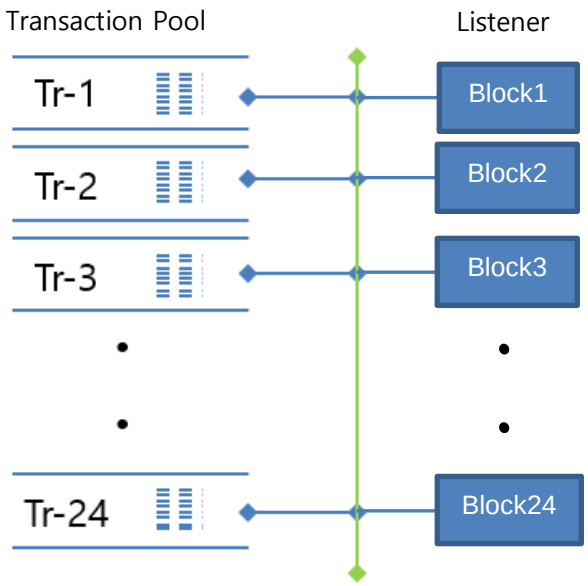
一般区块：1个区块为4MB。
特殊区块：3个特殊区块的容量具可变性，通过Cubing形成一般区块时生成。
CUBE的大小：特殊区块无规定大小，表示为 α。
1个CUBE = 24区块*4+α，即1个CUBE的大小为96+α MB

**数据到达交易池至生成CUBE的过程**

当交易明细或其他信息(输入数据的类型可以多样化，但所有数据必须经哈希(加密化)处理，其数据的长度和大小相同)到达交易池，Tr1~Tr24的数据将交易池里依次有序的进行分配，并生成一般区块。特殊区块在前CUBE生成的同时，复制并优先处理前CUBE的特殊区块。


Parallel Processing for TPS, Block Generation, Confirmation
Data Block Mining
Cube Mining (Cubing)
Special Block mining
tp#1
tp#2
tp#3
tp#4
tp#23
tp#24
TR
BK
Indexing Block
Address+No.Transaction+No.Block
Statistics Block
Condition { Address }
Escrow Block
Address { Address, Condition }
Concurrent Computing

[ 图 5 ]


Transaction Pool
Listener
Tr-1
Tr-2
Tr-3
Tr-24
Block1
Block2
Block3
Block24

[ 图 6 ]

每个区块的最大值为4MB，但根据情况也可能小于4MB。假如，大小小于4MB时，数据进入交易池的顺序为区块顺序，1个交易被分配给1个区块，以这种方式形成并列处理。挖矿者可以在资源允许的情况下，在24个区块中进行重复选择，参与挖矿。例如，在24个一般区块中选择2号、3号区块进行挖矿，也可选择特殊区块来挖矿。

### 2.5 POH (Proof of POW+POS hybrid)

采用POW+POS混合方式，促进矿工参与网络并减少耗电。POW与POS的混合使用可导致POS计算时间长等弊端，采用Statistics区块的统计功能可解决计算上的缺点，并确定POW和POS比率。对于钱包内持有5,000个以上Cube Chain者将赋予POS参与资格，并根据符合条件的对象的钱包持有量进行币奖励。
POH是POW和POS的混合方式，POW既是一种合约(在计算机之间交换信息时，对其通信方法的规则与承诺)，也是一个程序函数。POW是Proof-of-Work的英文缩写，表示工作量证明机制。
POW可视它为一个系统，持哈希(Hash)量越多，就可以找到更多的区块来获得币。这是一种影响思绪的经济手段，拒绝服务攻击和服务滥用(如网络上的垃圾信息)及通过要求几项操作来拖延处理时间。
目前，可开采的币大部分为POW方式。比特币、莱特币、狗币等以算法获得币奖励为概念的所有币均为POW方式。加密货币是从POW比特币开始的，至今主流币依然是POW币，POW市场规模远远超越了POS。POS方式有效解决了POW的问题，其一，节省了大部分成本和维护费用(电力和购买设备)；其二，解决了哈希垄断所导致的安全问题。POS只需准备一台连接网络的PC，无需附加更好的CPU和GPU。各个币的币奖励方式和数量均不同，但基本为POS持有量越多，可持续获得的币就越多。(类似利息的概念)
POS(Proof of Stake)如名字一样，持有整个币大量股份(Stake)者，可以从追加发行的币中获取大额份量。在POW中，如果'哈希'具有此功能，POS是'币'持有量基准。所以，POS方式为了安全，仅凭个人持币和与钱包的互连就可以形成超强的防护，无需大规模的哈希。另外，初期在短时间内发行大量币，可确保长期适量发行，这意味着大幅上涨或下跌的可能性极少。再者，无需消耗大量电力和挖矿机， 从而使更多人接触硬币、使用币。可是价格上涨幅度不大，所以存在几项弱点：没有'大量资金'流入；'资金'雄厚者很容易垄断；通过股份带来的利益比POW少；初期币的分配不公平等。

CUBECHAIN的POW与POS的初始比率为7:3，随着时间的推移POS比率逐渐提高，促使最终仅用POS来维持。以初期提高POW构建稳定的网络，随后逐渐提高POS减少网络资源和电力浪费。POW与POS的混合使用可导致POS计算时间长等弊端，若采用Cube Chain的Statistics区块，可有效减少每次重复计算的低效率性。最初，挖矿者起着促进生态系统的作用，提高了POW的比重，但它存在严重的资源浪费和通过竞争增加低效率的问题。所以，最初提高POW后，再进行逐渐调整，可促使最终仅维持于POS。及时分配POW和POS的优点，以获取适当的优势。

## 3. 加密化方式

### 3.1 钱包的生成

钱包生成最常用的方式为非对称(公开密钥和私有密钥)加密方式。 非对称加密方式将两个钥匙，以成对方式存在，如果用一个密码进行加密化，那么另一个钥匙进行解扰。两个密钥中，公开密钥在钱包生成

时用于钱包地址，私有密钥用于转账时的密码。Cube Chain在生成钱包地址和密码时，采用非对称加密方式(Asymmetric Cryptographic Technique)的RSA (Rivest Shamir Adleman，公钥加密)算法。

### 3.2 数字签名

通过钱包进行转账时，需要数字签名的过程，此时采用的加密方式为对称加密方式(Symmetric cryptographic technique)的AES256。

生成钱包地址和密码的RSA算法的非对称加密方式，虽然解决了密钥暴露也无法被破解的密码传递问题，但速度迟缓为弊端。尽管密钥的交换有难度，但结合了加密和解密速度快的AES256方式，完善了RSA的不足。

对于小数据，使用RSA生成的公钥与私钥作为生成数字签名密钥，改善数据加密化处理方式并非有效，但随着数据的变大，其改善效率性也将大幅度的提升。

### 3.3 区块哈希函数

哈希函数是将数据转换为任意长度的哈希值并输出的函数。转换后的数据不能用于恢复原始数据的解密，仅用于验证数据的完整性及对密码的验证。在区块链中，第n个区块的哈希值与第n-1个区块的哈希值相连。在Cube Chain中，相应区块内的27个区块都将生成各自的哈希值。此时，数据区块的哈希函数将使用SHA-256。

特殊区块与一般数据区块相比，数据将逐渐递增，所以必须使用与现有哈希函数不同的哈希函数。因此，将使用自主研发的CH-S1函数。如果使用现有的哈希函数将导致严重的速度迟缓。为此，将在数据输出/压缩过程中使用CH-S1函数来大幅提高哈希处理速度。

### 3.4 Cubing哈希函数

在进行Cubing时，采用的加密方式为自主研发的CHF(Cubing Hash Function Algorithm)算法。CUBE内的27个区块根据各自所处的不同位置，相邻的区块也不同。根据六面体的各面位置， 构成不同的结构。其结构为：角落8个、中心6个、环绕中心区块12个、正中央1个。4个结构均采用不同的哈希函数，分别命名为CH-B3、CH-B4、CH-B5、CH-B6。前面的CH(Cubing Hash) 表示为Cubing哈希函数，后面的B(Block) 表示为所处区块的CUBE内相邻区块数。Cubing哈希函数利用相邻区块的哈希值可生成新的哈希值。这样，27个区块均获得各自的哈希值。Cubing哈希值与区块哈希值的区别在于不是基于区块数据，而是基于相邻区块哈希值。通过Cubing哈希值验证现区块和整体区块，且27个区块创建独立链关系进行验证。根据CUEB内的位置值，进行相邻区块的相互验证，如有一个区块数据不符，将导致所有值的变动。

### 3.5 Cube 哈希函数

利用通过Cubing获取的27个区块的哈希值，生成整个CUBE的哈希值。 整个CUBE的哈希值与整个区块的哈希值生成现区块的CUBE哈希值。生成CUBE哈希值采用SHA-384函数。

## 4. 特殊区块的生成过程

### 4.1 特殊区块的设置

Cube Chain不仅仅是数据的移动，它还将对数据领域和特殊功能数据进行区分并予以扩展。为加密货币特别设置了3个特殊区块，但根据其他应用程序开发所需，可以通过Genesis文件对特殊区块进行另行设置。特殊区块的设置仅限在安装核心时使用，此设计易于各种领域的应用。另外，Cube Chain还准备了各种功能的特殊区块，今后还将陆续增加。

### 4.2 特殊区块的种类

特殊区块分别为Indexing区块、Statistics区块、Escrow区块、Format区块、Edit区块等。其中前3个区块在前已阐述，在此略过。

**Format区块**

Format区块是用于将要写入数据区块的数据格式化的灵活转换。如果更改格式化信息，Format区块将自动对数据进行有效性验证，从而防止错误数据的嵌入及用户或程序的出错。仅存储数据格式的数据，用户的一般数据不予使用。

**Edit区块**

Edit区块用于对现有数据的编辑。区块链的不可逆性既是优点也是缺点。虽然是加密货币中的基本要素，但在其他应用服务中有可能需要对数据进行编辑。为此，可以对Edit区块进行设置，使易于编辑、便于管理。
将要编辑的数据放入Edit区块中，并且在参照原始数据时，提供并反映Edit区块中的数据。区块链的数据不仅仅是简单的交易明细， 而是按照将参照值连接和断开，以便编辑好消除，从而而已对数据进行编辑。

特殊区块中Format区块和Edit区块是面向寻求私人区块链的机构或企业。如果，在24个区块中将2个区块转换为特殊区块，那么数据区块将变为22个。事实上，这并非是对区块链数据的编辑，而是将编辑对象添加到数据中，可理解为参照数据区域的位置产生了变化。即，将数据转换为可用于服务或应用程序，而并非对基础数据的编辑。Edit区块和Format区块与发行Cube Chain(QUB)没有连带关系，它们是一个选项型特殊区块，可以根据服务提供商的要求进行添加。

### 4.3 特殊区块的生成过程

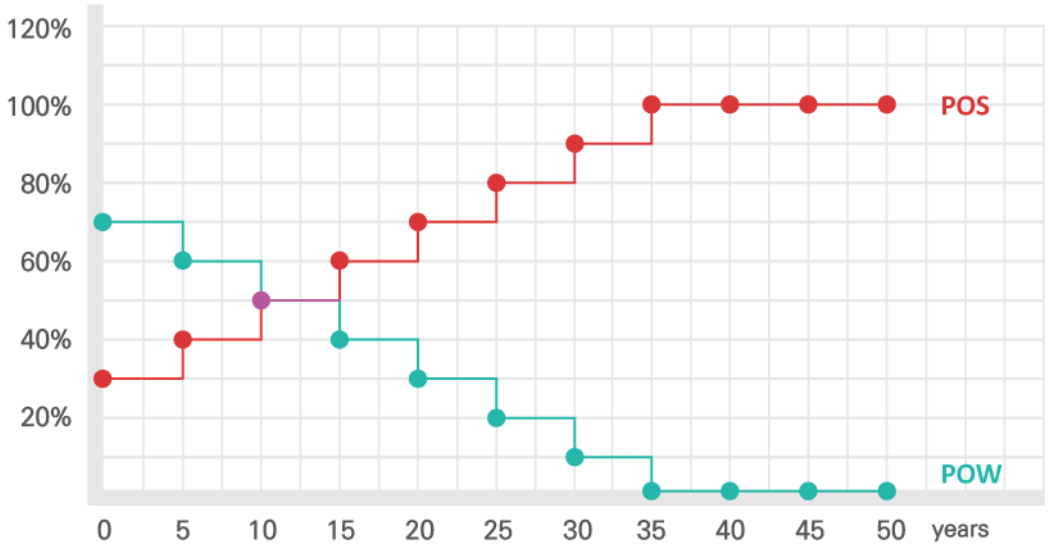
特殊区块基于数据区块，是重组数据或反映数据。3个指定特殊区块可视为数据区块的重组数据。为生成特殊区块，则必须要有前数据区块。因此，第一个CUBE将无法生成特殊区块。特殊区块的生成由第二个CUBE开始。特殊区块是在前CUBE完成生成时同时生成，并且与现CUBE数据区块完成生成时，一同形成Cubing。该过程是为了防止由生成特殊区块而导致Cubing 时间延迟的问题。特殊区块所反映的内容包含前CUBE的特殊区块数据中提取的内容和前数据区块的内容。

即，第n个CUBE的特殊区块包含截止到第n-1个CUBE的数据。在第n-1个CUBE完成时，包含第n-2个CUBE数据的特殊区块和第n-1个数据开始相结合，在形成第n个Cubing时，将与数据区块形成有机关系。特殊区块是在CUBE生成且CUBE与CUBE互联时段生成。虽然功能元素被扩展，但无时间延迟。另外，特殊区块采用的加密化技术为自主研发的CH-S1函数，与数据量相比可以快速获取哈希值。

## 5. 协议方式

### 5.1 POH (Proof of POW+POS hybrid)

Cube Chain的基本挖矿方式为POW，对参与工作证明的节点给予币奖励。为能有效解决因POW网络资源过度浪费及过度竞争而导致难度上升的问题，将采用结合POS奖励方式的POH(Proof of POW+POS hybrid)方式。
专属Cube Chain的POH方式可实现POW与POS 的同步进行，并且逐渐提高POS比率。这是为了有效防止因POW引起的工业化挖矿和网络资源浪费。




**[ 表格 1 ]**

参与POW挖矿有3种方式：生成数据区块、生成特殊区块、Cubing操作时根据各个项目进行选择性参与。

### 5.2 POW 奖励方式

参与工作证明的节点在每个CUBE生成后，进行相应计算并给予支付。
重复参与的情况下， 重复计算而支付，并对每个项目进行合算，给予支付。

- 在数据区块生成时，通过执行操作以查找添加到哈希值的随机值来获取奖励。此时，将对24个数据区块分别进行奖励，重复参与时给予重复奖励。
- 在每个特殊区块生成时，通过执行对哈希值的验证来获取奖励。
- 在Cubing过程中，通过执行对Cubing使用的加密化函数的验证来获取奖励。
- 由24个一般区块、3个特殊区块和1个Cubing组成，将分别给予奖励，重复参与时给予重复奖励。

### 5.3 数据区块的挖矿过程

- 确认区块的时间戳与相应节点的难易度。
- 将区块的时间戳与前区块的时间戳相比较，确认其有效范围。
- 创建区块中包含的数据或交易的相关列表。
- 确认区块Header的Merkle Tree(默克尔树)及有效性。
- 在前CUBE，连接相关区块的哈希值，生成首个哈希值。
- 采用前CUBE的模式区块，生成第2个哈希值。
- 生成区块，将区块数据传播至节点。

### 5.4 特殊区块的挖矿过程

特殊区块的挖矿方式为Cube Chain专属方式。其过程如下:

- 确认特殊区块的时间戳及相应特殊区块的Header。
- 在数据区块中提取要添加到特殊区块中的数据。
- 将数据的数量以项目种类划分，计算小计和总计。
- 构建此运算的Merkle Tree，并确认其有效性。
- 在前CUBE，连接相关区块的哈希值，生成首个哈希值。
- 采用前CUBE的模式区块，生成第2个哈希值。
- 将要添加的数据置入至前特殊区块中。
- 生成区块，将区块数据传播至节点。

### 5.5 Cubing的挖矿过程

Cubing的挖矿是为了一个称为CUBE化的独特方式的数据结构化。其过程如下:

- 确认前CUBE的时间戳及27个区块的哈希值。
- 将CUBE的时间戳与前CUBE的时间戳相比较，确认其有效范围。
- 确认27个区块哈希值的有效性。
- 确认27个模式区块哈希值的有效性。
- 利用前CUBE哈希值和27个区块哈希值，生成CUBE哈希值。
- 生成CUBE，传播到节点。

### 5.6 挖矿方式的多样化

Cube Chain的挖矿方式不仅多样化，并根据选择的各方式，其挖矿的效率性和难易度也略有不同。POW的使用旨在Cube Chain初始网络配置的流畅，并扩大参与范围，促使不同的参与者参与。可通过挖矿软件参与，并需要决定参与数量和挖矿区块。计划通过开发挖矿所需的解码的芯片或硬件设备来提高操作效率。这样，不仅可以实现低成本、高效率的挖矿，同时也克服了无限投资过热竞争的挖矿设备的低效率性。

### 5.7 POS 奖励方式

POH是Cube Chain专属的参与方式，其结合了POW挖矿方式和POS奖励方式。
无论节点是否参与，Cube Chain可直接在钱包内参与挖矿。将以前区块为基准，对持有5,000个以上Cube Chain(QUB)者余额保有人，按其持有数量比例给予分配。但，参与POS的数量，在参与期间不可转移， 参与数量以外的均可用于转账操作。支付时间为现区块生成时，支付数量将根据整体数量与持有数量比例支付。Cube Chain的Statistics区块内存有每个区块的POS对象的持有数量，由此可以快速计算奖励数量，并将其发送至每个钱包地址上。

## 6. 钱包服务

Cube Chain旨在使区块链服务变得更加便捷、更加实用。为此提供基本服务并扩展Cube Chain领域，创建一个可专注于开发应用程序或服务的环境。

### 6.1 钱包的提供

Cube Chain钱包支持使用Cube Chain的转账及交易明细管理等服务。Cube Chain钱包除了提供基本的转账、查询交易明细服务以外，还将提供多种特色性的钱包服务。作为引领第四次产业革命的新金融服务，Cube Chain将展现Cube Chain钱包专属形象，使应用程序的运用更加广泛、更加便捷。

#### 钱包地址的域名服务

钱包域名服务是将复杂难记的钱包地址与用户易于记忆的特定钱包名称相匹配的服务。如同将特定IP地址与指定域名地址进行连接一样，将用户指定的钱包域名地址与特定钱包地址相连，提高其便利性。钱包域名可使用易于记忆的个人手机号码或电子邮箱地址，轻松易记的钱包域名地址便于用户或转账者进行输入。

例）CWxhQRgBrqZUbj6fj1ftprurb2U9yAFMhu形式的Cube Chain地址

用户可以任意选择一个简单的字符串，如Abc.com(大小写均可)来代替复杂的钱包地址，并在Cube Chain中使用。即，可以通过Abc.com进行币的传输。

#### 钱包分组服务

这是一个将多个钱包捆绑在一个钱包的分组服务，通过仅公开连接钱包地址的形式，保护主钱包地址不被暴露。用户将通过一个钱包管理多个连接的钱包地址，可以根据使用目的开设多个钱包或分类使用。运用分组服务可进行自动转账，更便于管理多个连接的钱包地址。

**自动转账服务**

自动转账服务是根据用户拟定的转账条件(收款人，收款钱包地址，金额，周期等)，周期性的向特定钱包地址转账的服务。如使用自动转账服务，则无需收款人的转账告知书，即可在指定日期将资金从钱包中提取并批量转入收款帐号，同时收到交易详单。

**钱包信息转达服务**

针对使用钱包用户，在交易完成时接收确认信息或关于服务请求的消息。信息服务可用于转账成功通知或交易出错要求退还等，此信息可通过应用程序的消息推荐、手机短信、电子邮件等方式接收。

## 6.2 基于Cube Chain的应用服务

基于Cube Chain的应用服务是指构建基本服务平台之后，再进行部署，以便基于区块链的Cube Chain技术运用于诸多领域的商业模型。目的在于无论是企业或个人都可以运用Cube Chain，从而形成一个良好的开发环境，创建更加广阔的Cube Chain生态系统，为第2代Cube Chain应用程序的发展奠定基础。基于Cube Chain的服务，该服务将被开发成可以直接应用于商业模型的完整形式，并将作为平板APP另行发布。

**Cube Chain个人信息验证服务**

这是一种个人验证服务，可使用Cube Chain存储常用的个人电子邮件、手机号码、PIN码等。用户可以将存储在Cube Chain上的个人信息提供于互联网或应用程序。存储于Cube Chain上的个人信息将基于数据保护，只在需要本人验证时公开，绝不泄露于第三方，确保与信息使用方的安全链接。

**Cube Chain信息服务**

基于Cube Chain的信息服务与现信息服务的不同之处在于它将以P2P方式进行。来往信息数据均由Cube Chain传输并存储。由于信息数据以次级存储，因此用户在数据传输上无时间延迟。Cube Chain数据的分布式存储有效保护用户隐私，信息仅提供于本人验证所需。隐私的保护及存储功能作为安全保护屏障，可防止第三方泄露及黑客攻击，为用户提供安全的聊天服务。此外，还可通过API开设聊天室、设定参与者、传递参与者的对话内容等，扩大其运用范围。

**Cube Chain文档保存服务**

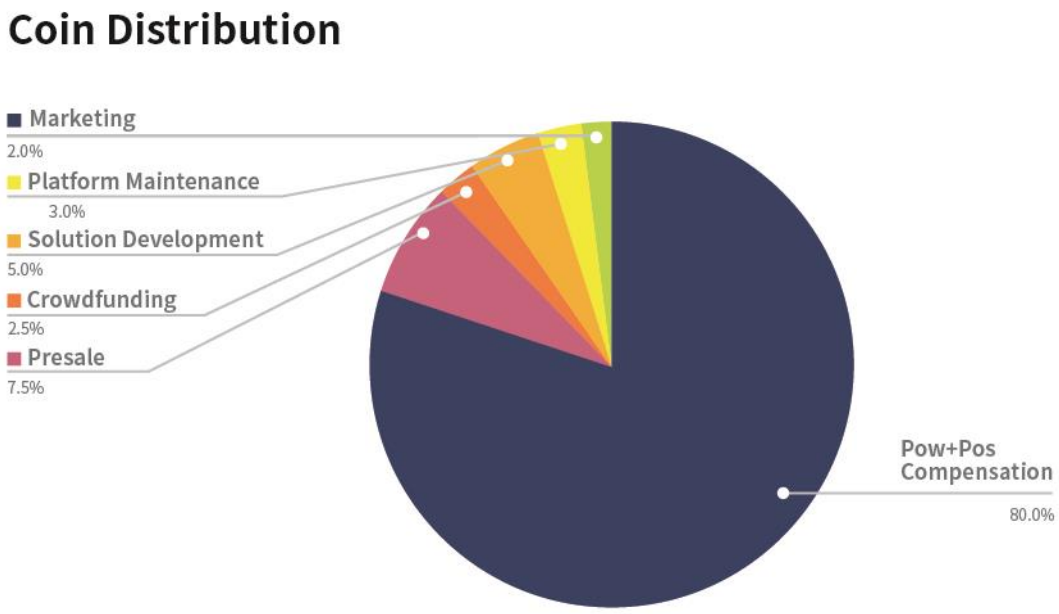
使用Cube Chain文档保存服务，用户可通过Cube Chain将特定文档进行分散存储，并根据情况设定特定文档为公用文档或认证文档。用户可通过此服务存储文本文件或图片文件，对重要文件进行安全保管。此外，还可以通过平板APP或与应用程序的互联服务提高文件的泛用度。

**Cube Chain数据库服务**

Cube Chain的数据库服务是为了提高区块链的数据如数据库一样被广泛运用。使用Cube Chain的Edit区块和Format区块，提供数据结构化管理。通过提供API，数据管理将采用标准SQL语句进行存储、编辑、删除。另外，还提供一种通过关系型数据库，在Cube Chain数据的CUBE生成时发送数据并予以联动的功能。

## 7. Cube Chain 发行数量

### 7.1 Cube Chain 分配




**[ 表格 2 ]**

### 7.2 POH 比率

Cube Chain在未来50年的总发行量为120亿个，POW与POS的比率定为5年一调整。

| 区分 | 5 年期间<br>Cube Chain<br>奖励数量 | POW : POS<br>比率 | 5 年期间<br>POW<br>奖励数量 | 5 年期间<br>POS<br>奖励数量 |
|---|---|---|---|---|
| ~5 年 | 960,008,400 | 7:3 | 672,005,880 | 288,002,520 |
| 5~10 年 | 960,008,400 | 6:4 | 576,005,040 | 384,003,360 |
| 10~15 年 | 960,008,400 | 5:5 | 480,004,200 | 480,004,200 |
| 15~20 年 | 960,008,400 | 4:6 | 384,003,360 | 576,005,040 |
| 20~25 年 | 960,008,400 | 3:7 | 288,002,520 | 672,005,880 |
| 25~30 年 | 960,008,400 | 2:8 | 192,001,680 | 768,006,720 |
| 30~35 年 | 960,008,400 | 1:9 | 96,000,840 | 864,007,560 |
| 35~40 年 | 960,008,400 | 0:10 | - | 960,008,400 |
| 40~45 年 | 960,008,400 | 0:10 | - | 960,008,400 |
| 45~50 年 | 960,008,400 | 0:10 | - | 960,008,400 |

**[ 表格 3 ]**

## 8. Cube Chain的技术运用

### 8.1 RPC服务器

参与Cube Chain的节点可以用作RPC服务器。如使用RPC服务器，可以远程运行函数，因此，运用Cube Chain可以远程操控节点。在构成Cube Chain网络的节点中使用RPC服务器，可操控不属于Cube Chain的PC或服务器查看Cube Chain的数据或节点。通过远程对目标进行权限设置或功能范围的设置，对全局实施远程监控。

### 8.2 API

Cube Chain将与RPC服务器一起API，促使远程可以轻松管理节点。RPC服务器的API传递和应答，基本使用JSON方式。详细的API文档计划在Cube Chain进行时公开。API的使用命令语及简单的例示如下:

**rpc_ver :** 获取RPC服务器的当前版本信息。
curl -X POST --data '{"callno":100,"com":"rpc_ver","vars":{},rmsg:"请求确认服务器版本"}'

**network_info :** 获取服务器的网络参与类型和参与节点及激活状态的相关信息。
curl -X POST --data '{"callno":100,"com":"network_info","vars":{},rmsg:"请求确认网络信息"}'

**p2p_info :** 获取p2p相关信息。
curl -X POST --data '{"callno":100,"com":"p2p_info","vars":{},rmsg:"peer to peer信息"}'

**cube_pow :** 获取有关POW参与的信息。
curl -X POST --data '{"callno":100,"com":"cube_pow","vars":{},rmsg:"确认POW状态"}'

**cube_pos :** 获取已传递的钱包地址的POS信息。
curl -X POST --data '{"callno":100,"com":"cube_pos",
"vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"确认POS状态"}'

**cube_height :** 获取当前链的高度，即目前为止CUBE的数量。
curl -X POST --data '{"callno":100,"com":"cube_height","vars":{},rmsg:"确认链数量"}'

**cube_balance :** 确认已传递的钱包地址的余额。
curl -X POST --data
'{"callno":100,"com":"cube_balance","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"}
,rmsg:"确认钱包余额"}'

**cube_transaction_count :** 确认已传递的钱包地址的交易次数。
curl -X POST --data

'{"callno":100,"com":"cube_transaction_count","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"确认钱包的交易次数"}'

**cube_transaction_list :** 提取交易的哈希值，即交易帐号。可查看特定地址的交易明细或特定CUBE高度的交易明细。
curl -X POST --data
'{"callno":100,"com":"cube_transaction_list","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"传输交易明细"}'

**cube_transaction_detail :** 传输交易的哈希值的详细信息。
curl -X POST --data
'{"callno":100,"com":"cube_transaction_detail","vars":{"tr_hash":"6e8dd67c5d32be8058bb8eb970870f072445675058bb8eb97f"},rmsg:"传输交易或数据"}'

**cube_transaction :** 在已传递的钱包地址之间进行交易。
curl -X POST --data
'{"callno":100,"com":"cube_transaction","vars":{"address_from":"Q9eeb85d32cf465507dd71d503d8a85d32s","address_to":"Qd2be8058bb8eb970870f0723315b60e8dd","amount":1.2,"fee":0.0001},rmsg:"传输交易或数据"}'

**cube_transaction_data :** 将特定数据加载到Cube Chain。
curl -X POST --data
'{"callno":100,"com":"cube_transaction","vars":{"address_from":"Q9eeb85d32cf465507dd71d503d8a85d32s","address_to":"Qd2be8058bb8eb970870f0723315b60e8dd","data":{"no":1,"id":"cubechain","chapter":"cubechain_api","book_name":"Cube Chain白皮书"}},rmsg:"传输一般数据"}'

## 9. 结论

区块链技术正在发展成为引领第四次产业革命的基础技术。坚信在不久的将来，它将成为大众化技术，不再仅限于加密化货币市场，而是遍布整个产业领域，同时确保数据的自由共享和安全性。Cube Chain致臻完善现区块链的缺点，为区块链技术发展发挥余热、贡献力量。竭力使Cube Chain成为引领第四次产业革命的领先技术，创新求发展，使其可广泛易用于诸多领域。