USB BIOCKCHAIN

咨询币区块链白皮书

SAXSON 资本集团：USB Blockchain 基金会 编著

目录

摘要

USB Blockchain （简称“咨询币”或“USB”）致力于开发比特币和以太坊之外的第三种区块链生态系统，通过价值传输协议（“Value Transfer Protocol”）来实现点对点的价值转移，并根据此协议，构建一个支持多个咨询和资讯行业（包括金融、物联网、供应链、社交、游戏等）的去中心化的应用开发平台（“DApp Platform”）。由于技术上的创新、治理结构完善、应用范围广，USB Blockchain 将成为优于比特币和以太坊的公链：

从技术角度分析，USB Blockchain 具有强大的开发团队，通过引入 Identity、Oracle 和数据馈送（Data feeds）机制，并兼容比特币改进协议（Bitcoin Improvement Proposals）的 UTXO 交易模型，实现了首个基于 IPoS（激励权益证明）共识机制的智能合约平台。在合规性方面，也符合不同行业的监管需求，其中部分顶尖技术团队来自以太坊的核心技术团队人才。

从治理角度分析，USB Blockchain 设立 USB Blockchain 基金会，致力于 USB Blockchain 的开发建设、治理透明度倡导和推进工作，促进开源生态社会的安全、和谐。通过制定良好的基金会治理结构，分别从代码管理、财务管理和公共关系等多个维度帮助管理开源社区项目的一般轶事和特权事项，从而确保 USB Blockchain 的可持续性、基金会内部管理有效性及募集资金的安全性。

从 USB Blockchain 应用角度分析，USB Blockchain 通过“去中心应用”和“主控合约”将链下因素引入，形成符合现实世界商业逻辑的区块链主控合约，支持多个行业、多种渠道，最终实现走向移动端策略

（Go Mobile）。在 USB Blockchain 的生态系统中，我们将会与第三方开发者一起，从技术架构支持提供移动端的服务，包括：移动端钱包、移动端 DApp 应用、移动端智能合约服务。我们也鼓励第三方的开发者加入我们，一起开发区块链的移动端服务，共同推动区块链技术的落地。

作为最有前景的区块链生态系统，USB Blockchain 完美地结合了比特币和以太坊的优点，并解决了现有区块链系统的固有缺陷。USB Blockchain 将持续通过基础平台的搭建，以及各产品的开发和商业化落地项目的发展和迭代，逐步形成区块链经济，提升全球咨询和咨询行业的效率，促进社会的高效协同发展。

USB Blockchain，咨询界区块链经济开创者。

第一部分 USB Blockchain 的设计理念

1.1 区块链出现的背景和意义

在比特币诞生之前，全球信息传递都是通过互联网的 TCP/IP（传输控制协议/因特网互联协议）协议来实现高速低成本的传输，但是随着互联互通技术的发展（互联网、物联网、VR/AR），人与物体、人与信息的交互方式更加多样化，更多的实体被数字化或者代币化，仅仅是信息的分享和传输并不能满足经济社会的发展，因此当实体被数字化或者代币化之后，人们越来越关注到价值转移以及如何点对点传输这些资产和价值。

在 2008 年 10 月 31 日，Satoshi Nakamoto 第一次发布了比特币的白皮书《比特币：一种点对点网络中的电子现金》，并提出了通过去中心化的比特币网络实现价值转移。在比特币体系中，全网参与者均为交易的监督者，交易双方可以在无需建立信任关系的前提下即可完成交易。区块链技术改变了我们获取和分享信息的方式，创造了一个新的分布式、点对点的生态社会。

在比特币网络出现之前，我们一直无法在不借助于第三方受信机构的情况下，通过互联网进行点对点的价值的转移和传输。比特币网络则是运行于信息高速公路上面的第一个 Value Transfer Protocol （“VTP 协议”）。在本白皮书中，我们也第一次归纳和提出了互联网应用层 VTP 协议的概念。

目前，随着区块链技术的成熟，区块链的应用场景不仅限于比特币和以太坊，USB Blockchain 试图将区块链链上和链下相结合，形成第三个区块链的生态环境，进一步使用 VTP 协议实现点对点价值传输。

1.2 为什么设计 USB Blockchain

自从 2009 年比特币代码开源以来，社区里面出现了很多代币和其他区块链项目，还包括致力于成为通用智能合约平台和去中心化应用平台的以太坊项目，但是区块链行业不论是从技术角度，还是行业应用角度都还面临着很多挑战。主要问题如下：

1. 缺乏新型的智能合约平台。比特币生态和以太坊生态由于缺少与现实社会的连结，使各行业的广泛应用受限；

2. 不同区块链平台之间的兼容性。比如基于 UTXO 模型的比特币生态和基于 Account 模型的以太坊生态无法兼容；

3. 共识机制本身缺乏灵活性。因为参与者的不同，在公有链中和联盟链中，对共识机制的要求不尽相同；

4. 缺乏对行业合规性的考虑。例如在金融行业要求的尽职调查，如背景调查和 KYC （“Know-Your-Customer”）部分，在现有的区块链系统中，难以实现；

5. 现有区块链系统具备很大的封闭性。目前大多数智能合约仅接受链上数据作为触发条件，缺乏与现实世界的交互。

而当然，我们还发现如今各个领域都有相应的团队在做区块链经济，没有行业标准和相关部门的规范的。而在比特币疯涨的魅力下，很多行业巨头也纷纷加入了这个行业。软银集团的董事长孙正义瞄准了 VR 虚拟交友区块链经济，腾讯瞄准了游戏虚拟装备区块链经济等等。而我们想要解决的是：全球咨询行业的区块链经济。

我们希望可以构建一个全新的区块链生态系统——USB Blockchain，咨询界区块链经济开创者。作为未来世界可选的互联网价值传输协议，并把整个区块链行业的易用性向前推进一步。我们将颠覆全球的咨询行业/资讯行业；在未来，我们的所有咨询服务收费将变革成区块链经济，让付费变成投资，让服务变成投资，让交易变成收益。

1.3 USB Blockchain 的设计原则

针对区块链技术和行业应用局限性的各种问题，USB Blockchain 提出的改进方案如下：

1. 引入全新设计的主控合约，通过链下数据和链上数据的共同输入作为触发条件，完成合约的执行；

2. 实现区块链技术之间的兼容性；

3. 面向公有链的灵活共识机制；

4.增加对行业合规性的考虑，提供可选的身份识别模块；

5.通过链下数据作为主控合约触发条件，实现与现实世界的交互。

除此之外，USB Blockchain 在开发过程中还加入了模块化的设计和易用性的考量。为了便于开发和维护，将 USB Blockchain 分为三大模块，分别为 USB Blockchain 技术模块、USB Blockchain 用户交互模块和 USB Blockchain 商业路径模块。

为了对应不同用户的操作系统和开发需求，同时也真正做到开源，我们提供不同版本的 USB Blockchain 系统，另外还提供移动端的服务，鼓励第三方的开发者，与我们一起推动区块链技术在中国的落地，开发出普通互联网用户可以使用的区块链移动端服务。

1.4 USB Blockchain 的愿景

USB Blockchain 致力于通过咨询行业、第三方开发者和技术上的创新，打造一个在全球具有影响力的开源社区生态，最终目的是将区块链融入到咨询行业的金融、社交、游戏、物联网等不同生态链。USB Blockchain 是有兼容性的生态社会，并且通过融入监管的逻辑，通过 Oracle 和 Data Feed 架起区块链与现实商业社会的桥梁。

技术上创新：USB Blockchain 打造的是一个安全可靠并且与以太坊社区和比特币系统兼容的平台，通过技术和理念上的创新实现链上与链下相结合。

可持续发展：为实现 USB Blockchain 的可持续性发展，避免散沙式的发展结构和底层构架分化，USB Blockchain 基金会将制定完善的治理架构，对一般轶事、代码管理、财务管理、薪酬管理和特权操作范围等事务进行管理。同时，治理架构会随着基金会和社区的发展不断更新，并引入监察和监督功能，规则制定和变更控制管理等。

商业应用：USB Blockchain 基金会将参考投行的做法进行行业分析和筛选，选择适当的行业推广 USB Blockchain 技术应用，让企业在 USB Blockchain 上进行开发和应用，同时也促进 USB Blockchain 的可持续发展。

合作伙伴：USB Blockchain 基金会通过与合作伙伴的通力合作，将企业、商界、技术和政府等多方面资源进行整合，最大化实现资源共享，最高效利用资源，实现社会协同发展。

USB Blockchain 基金会还将提供透明的财务管理，全面的代码管理并协助 USB Blockchain 进行商业落地。同时，基金会将保持高标准的诚信和道德的商业行为，遵守相关的法律法规。此外，USB Blockchain 基金会将聘用第三方机构提供相关工作审计报告，合规治理和监督。

为进一步使 USB Blockchain 成为完全开源社区生态，USB Blockchain 基金会最终将 80%的咨询币发放给社区，用于商业应用、市场推广等帮助实现真实世界与区块链世界的结合，剩余 20%咨询币奖励创始团队、早期投资者、顾问和开发团队。

从 USB Blockchain 的雏形阶段、开发阶段到正式推出，得到了包括创始团队、开发团队、行业专家、早期投资者、律师和咨询顾问等社会各界的大力支持。

第二部分 USB Blockchain 技术特征

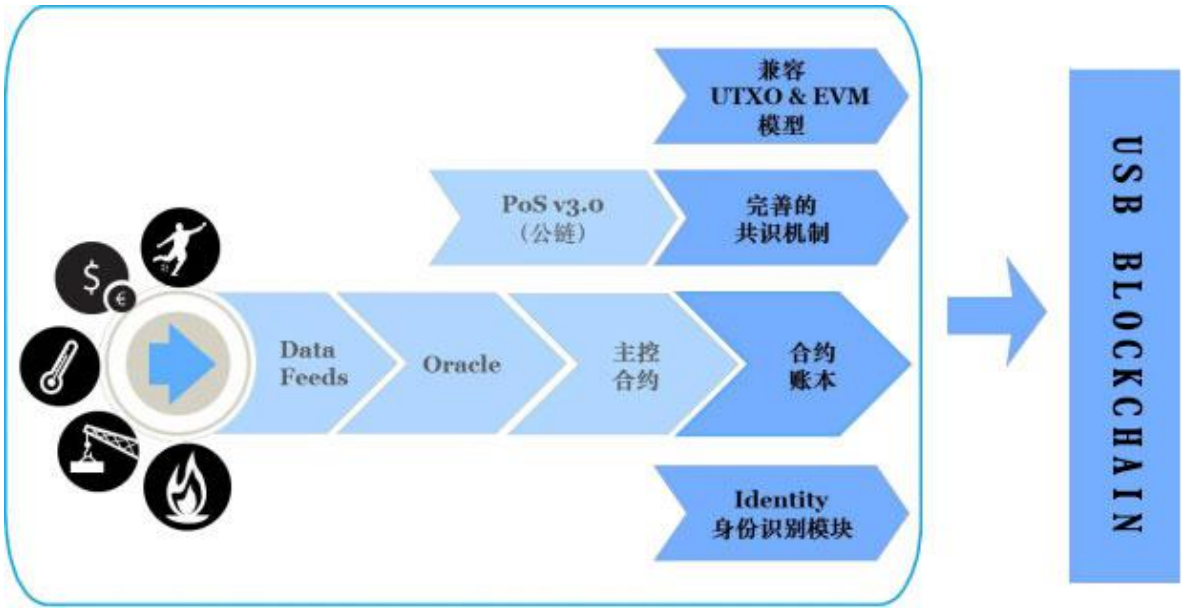
2.1 USB Blockchain 概述

USB Blockchain 致力于开发兼容比特币和以太坊的全新生态系统，并且以行业应用为导向，通过移动端 DApp 开发策略，把区块链的技术优势带给不同行业的应用者和普通互联网用户。

另外 USB Blockchain 更加注重智能合约的实际应用，将通过完善的 Oracle 和 Identity 模块的设计，并加入了数据馈送（DataFeeds）机制，使得传统互联网企业（金融、物联网等）应用区块链技术时满足相关合规性的要求。

除此之外，USB Blockchain 还将重点开发去中心化应用，与第三方开发者一起，为普通用户提供移动端的去中心化应用，共同携手打造 USB Blockchain 生态系统。

2.2 USB Blockchain 模型



兼容 UTXO 和 EVM

一方面，USB Blockchain 采用了 UTXO 模型保证交易的连续性和可溯源性。另一方面，以太坊的智能合约均可在 USB Blockchain 上运行。因此，USB Blockchain 完美的结合了比特币和以太坊的优点，并解决了两者的固有缺陷。

共识机制

我们使用了 Proof of Stake 作为USB Blockchain的共识机制。在后续的开发过程中，我们计划在 POS 基础上添加激励措施和估计节点在线，并称之为激励权益证明共识机制（IPoS）。

合约账本

在USB Blockchain中，合约账本存储了所有的USB Blockchain明文可读性强的合约内容，用户可以选择性地

把自己感兴趣的合约代码和合约解释通过 P2P 的形式下载到自己的USB Blockchain 客户端。合约账本的构建，可以给 USB Blockchain 系统中的合约带来更多的透明性、可读性以及可审计性。

首先，链下数据作为 data feeds 输入到USB Blockchain上，然后Oracle 选择合适的数据触发智能合约。为了避免 The DAO 事件的再次发生，我们还在USB Blockchain中引入了监管者的角色。

Data Feeds:

Data Feed 代表任何从链外取得的数据，比如汇率、GDP、某个城市的温度、比赛结果等。然后将数据输入到智能合约或者去中心化应用。

举个例子，当房间里的温度降到 10 摄氏度以下时，空调将自动转化为“制热”模式。这里，温度计上的读数就是链外数据。

Oracle:

在 USB Blockchain 系统中，Oracle 代表可信的特定的机构、实体、节点、公钥地址。当有多个数

据源时，Oracle 可以根据预先制定的规则选择合适的数据输入USB Blockchain。

主控合约:

在以太坊中，只有链上数据可以触发智能合约。在 USB Blockchain 中，我们引入了链下数据，与链上数据一起作为触发条件，完成合约的执行。这样的智能合约我们称之为主控合约。

Identity 身份识别模块

正如我们所知，金融行业对数据的安全性和身份识别有更加严格的要求。我们在 USB Blockchain 上引入了第三方征信机构，通过 Identity 身份识别模块验证的客户，将获得更多的权限。

2.3 USB Blockchain 合约实现方式

用合约来实现交易的代码是这样的：

```
[

nonce,

'',

value,

[

data item 0, data item 1,
...

],

v,

r, s

]
```

在大多数情况下，数据项会是脚本代码（后面有更多解释）。来用创建合约的交易是这么验证的：

把交易反串行化，然后从它的签名里提取发送地址。

计算出交易费，确保创建者的账户金额不少于“捐助额+交易费”，如果不是，则退出；如果是，支付交易费。

对于创建合约的交易， 从它 RLP 编码的 sha3 哈稀值中至少提取最后 20 位，如果与这个地址关联的账户已经存在了，则退出；如果不是，则为这个地址创建合约。

为[0 ... n-1]范围的每一个 I，拷贝数据项 i 到合约的数据槽 i，n 是交易里数据项的总数。

代码语言详述

合约的脚本语言是汇编语言和比特币的基于堆栈的语言的混合体，它里面总是保有一个指数指针，通常每完成一步执行指针就往前走一位，如果指针保持原位则操作会被连续执行。所有的操作符都是[0…63]之间的数，除非这里有特殊说明的操作符，如 STOP、EXTRO
BALANCE 这些，它们后面还要定义数值。这种脚本语言可以访问三类存储：

堆栈——一种暂时存储，每当合约执行完成，它的列表就会被清零。对于堆栈通常的操作是在其顶部加进或移除数值，所以在程序执行过程中它的长度会增大或缩小。
内存—密钥或数值的暂时存储，每当合约执行完成，它就重置为“0”。密钥和数值以[0…2^256-1]之间的整数形式存储。
存储—密钥或数值的永久存储，它的初始值是零，除非是合约刚建立的时候插入的一些脚本代码。当它在帕特里夏树里编码时，所有的密钥和数值都以大字节序编码存储，而一个含“0”的密钥则表示这把密钥不在帕特里夏树里。密钥和数值以[0…2^256-1]之间的整数形式存储。
每当一笔交易被发送到某个合约，合约就执行它自己的脚本代码，具体的步骤是这样：
增加发送的咨询币数额到合约的账户金额

指数指针设为零，还有 STEPCOUNT = 0
永久重复：

o 如果在指数指针处的指令是 STOP、非法、或者大于 63，跳出循环。 o 令 MINERFEE = 0，VOIDFEE = 0、

o 令 STEPCOUNT <- STEPCOUNT + 1

o 如果 STEPCOUNT > 16，令 MINERFEE <- MINERFEE + STEPFEE

o 查看指令是不是 LOAD 或 STORE，如果是，令 MINERFEE <- MINERFEE + DATAFEE o 查看指令会不会装满空的内存域，如果会，令 VOIDFEE <- VOIDFEE + MEMORYFEE o 查看指令会不会清零已用的内存域，如果会，令 VOIDFEE <- VOIDFEE - MEMORYFEE

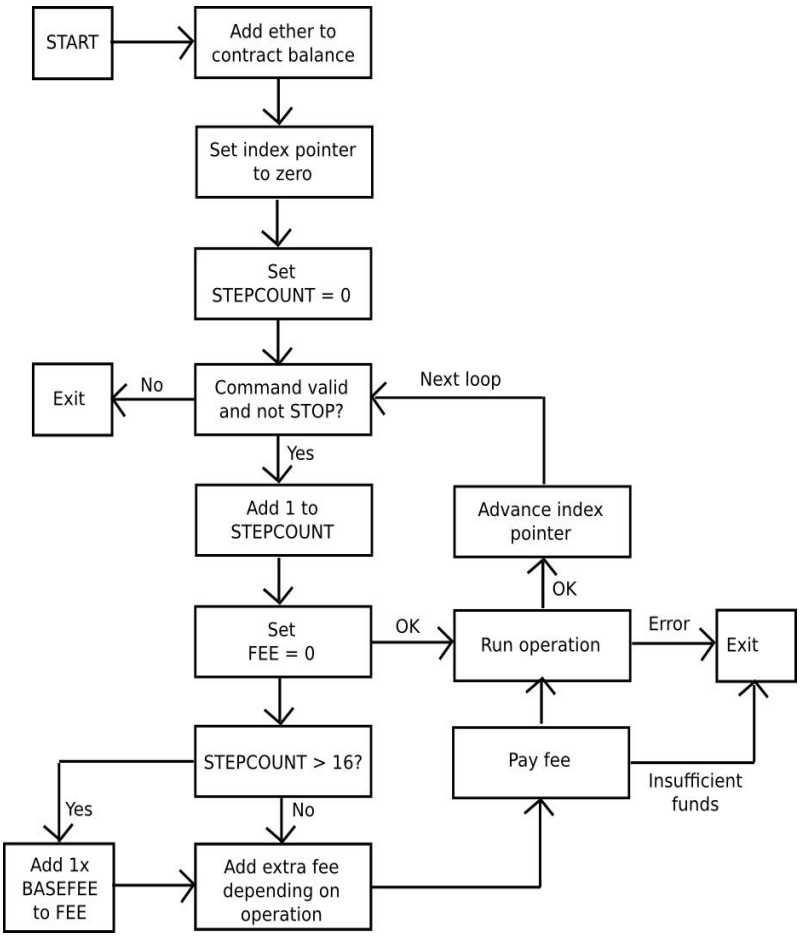
o 查看指令是不是 EXTRO 或 BALANCE，如果是，令 MINERFEE <- MINERFEE + EXTROFEE o 查看指令是不是密码运算，如果是，令 MINERFEE <- MINERFEE + CRYPTOFEE o 如果 MINERFEE + VOIDFEE > CONTRACT.BALANCE，暂停并跳出循环。

否则，从合约的账户金额里减去 MINERFEE + VOIDFEE，并把 MINERFEE 加到一个运行中的计数器，计数器的金额会在所有交易都分列完成后加到矿工的账户金额上。注意，在有的情况下 MINERFEE 可能是负数，那么合约的账户金额是增加的。

o 执行命令

如果命令没有因出错而跳出，那就更新指数指针并回到循环的起点。如果命令因出错而跳出，终止循环。注意，如果合约因出错而跳出，这并不会使交易或区块非法，而只表示合约没执行完就停了。

合约脚本阐释



在以下描述中，S[-1]、 S[-2]等等表示堆栈最顶端、第二顶端的项。各个操作符定义如下：

(0) STOP - 停止执行

(1) ADD - 弹出两项并压入 S[-2] + S[-1] mod 2^256 项

(2) MUL - 弹出两项并压入 S[-2] * S[-1] mod 2^256 项

(3) SUB - 弹出两项并压入 S[-2] - S[-1] mod 2^256 项

(4) DIV - 弹出两项并压入 floor(S[-2] / S[-1])项，如果 S[-1] = 0，停止执行。

(5) SDIV - 弹出两项并压入 floor(S[-2] / S[-1])项，但把超出 2^255 的部分看作负数 (也就是 x -> 2^256 - x)。如果 S[-1] = 0，停止执行。

(6) MOD - 弹出两项并压入 S[-2] mod S[-1]项。如果 S[-1] = 0，停止执行。

(7) SMOD - 弹出两项并压入 S[-2] mod S[-1]项，但把超出 2^255 的部分看作负数 (也就是 x -> 2^256 - x)。如果 S[-1] = 0，停止执行。

(8) EXP - 弹出两项并压入 S[-2] ^ S[-1] mod 2^256 项

(9) NEG - 弹出两项并压入 2^256 - S[-1]项

(10) LT - 弹出两项并压入 1，如果 S[-2] < S[-1]；否则压入 0

(11) LE - 弹出两项并压入 1，如果 S[-2] <= S[-1]；否则压入 0

(12) GT - 弹出两项并压入 1，如果 S[-2] > S[-1]；否则压入 0

(13) GE - 弹出两项并压入 1，如果 S[-2] >= S[-1]；否则压入 0

(14) EQ - 弹出两项并压入 1，如果 S[-2] == S[-1]；否则压入 0

(15) NOT - 弹出两项并压入 1，如果 S[-1] = 0；否则压入 0

(16) MYADDRESS - 把合约地址当作数字压入

(17) TXSENDER - 把发送者的地址当作数字压入

(18) TXVALUE - 压入交易金额
(19) TXDATAN - 压入数据项的总数

(20) TXDATA - 弹出一项并压入数据项 S[-1]；如果指数溢出范围，则压入 0

(21) BLK_PREVHASH - 压入前一个区块的哈稀值（不是当前区块，因为这没有可能）

(22) BLK_COINBASE - 压入当前区块的币基（coinbase）

(23) BLK_TIMESTAMP - 压入当前区块的时间戳

(24) BLK_NUMBER - 压入当前区块的号数

(25) BLK_DIFFICULTY - 压入当前区块的难度值

(26) BASEFEE - 压入基准费用（乘以，以下费用章节会作定义）

(32) SHA256 - 弹出两项，然后把内存里处于从指数 S[-2] 到(S[-2] + ceil(S[-1] / 32) - 1) mod 2^256 的所有 ceil(S[-1] / 32)项都提取出来，用它们来生成一个字符串，如有必要，填充“0”字节使得他们的长度是 32 字节，再提取最后的 S[-1] 字节。压入字符串的 SHA256 哈稀值。
(33) RIPEMD160 - 跟 SHA256 一样执行，只不过用的 RIPEMD-160 哈稀。

(34) ECMUL - 弹出三项。如果(S[-2],S[-1]) 是在 secp256k1 曲线上合法的点，包括两个座标都要小于 P，则用(0,0)作为无穷处的点，压入(S[-2],S[-1]) * S[-3]项进堆栈；否则压入(2^256 - 1, 2^256 - 1)。注意这里对 S[-3]并无限制。

(35) ECADD - 弹出四项，压入(S[-4],S[-3]) + (S[-2],S[-1])，如果这两个点都合法；否则，压入(2^256 - 1,2^256 - 1)。

(36) ECSIGN - 弹出两项，压入(v,r,s) 。这里，(v,r,s) 是哈稀 S[-1]的 Eletrum 类型的 RFC6979 决定性签名，此时私钥是 S[-2] mod N 。

(37) ECRECOVER - 弹出四项，把(x,y)作为公钥压入，这个公钥来自于哈稀 S[-4]的签名(S[-3],S[-2],S[-1]) 。如果签名里有 v,r,s 的值非法（也就是说，v 不在[27,28]里，r 不在[0,P]里，s 不在[0,N]里），则返回(2^256 - 1,2^256 - 1)。

(38) ECVALID - 弹出两项，如果(S[-2],S[-1]) 是 secp256k1 曲线上合法的点（包括(0,0)），则压入 1；否则，压入 0。

(39) SHA3 - 跟 SHA256 一样执行，只不过是 SHA3 哈稀，256 位版本。

(48) PUSH - 在指数指针+1 处压入项，并让指数指针前进 2。

(49) POP - 弹出一项。

(50) DUP - 压入 S[-1]进堆栈。

(51) SWAP - 弹出两项，先压入 S[-1]，再压入 S[-2]。

(52) MLOAD - 弹出一项，再把它压入至内存里的指针 S[-1]处。

(53) MSTORE - 弹出两项，把内存里的指数 S[-1]设为 S[-2]。

(52) SLOAD -弹出一项，再把它压入至存储里的指针 S[-1]处。

(53) SSTORE -弹出两项，把存储里的指数 S[-1]设为 S[-2]。

(54) JMP - 弹出一项，再把指数指针设为 S[-1]。

(55) JMPI - 弹出两项，只有当 S[-1] 不为零时，把指数指针设为 S[-2]。

(56) IND - 压入指数指针。

(57) EXTRO - 弹出两项，压入合约 S[-1]的内存指数 S[-2]。

(58) BALANCE - 弹出一项，压入地址的账户金额；如果不是地址，则压入 0。

(59) MKTX - 弹出四项，发起一个交易发送 S[-2] 个咨询币到 S[-1]，同时带 S[-3]个数据项。把在内存里从指数 S[-4]到指数(S[-4] + S[-3] - 1) mod 2^256 的项作为交易的数据项。

(63) SUICIDE - 弹出一项，销毁合约并清空所有存储，从正在清空的内存发送全部的账户金额另加负数的费用到位于 S[-1] 处的地址。

如上所述，我们不是要让人们直接写 USB Blockchain 脚本，而是发布编译器从高级语言来生成 USB Blockchain 脚本。头两个编译的目标很可能会是之前描述的类 C 语言，而第二个是更全面的头等函数语言，它会支持数组和任意长度的字符串。对于编译器来说，编译类 C 语言比较容易，变量可以被指定到内存指数，编译算术运算符会复杂一些，其方式是转化为反向波兰表示法（例如，(3 + 5) * (x + y) -> PUSH 3 PUSH 5 ADD PUSH 0 MLOAD PUSH 1 MLOAD ADD MUL）。头等函数语言因为变量辖域而更复杂，可能的解决办法在内存里是保留一份连接着的堆栈框架的列表，通过给每个堆栈框架 N 个内存槽来实现，这里 N 是程序里不同变量名的数量。获取变量的方法分以下几步：从上到下搜索堆栈框架列表直到有一个框架包含指向变量的指针；为了记住，拷贝指针至堆栈框架的顶部；然后在指针处发回数值。然而，这些属于长远考虑，因为编译与真正的协议是分离的，所以等网络运行起来很久之后再来研究编译策略都是可能的。

2.4 USB Blockchain 的创新实现方式

USB Blockchain 的设计将遵循以下原则：

1.简洁原则 - USB Blockchain 协议将尽可能简单，即便以某些数据存储和时间上的低效为代价。一个普通的程序员也能够完美地去实现完整的开发说明。这将最终有助于降低任何特殊个人或精英团体可能对协议的影响并且推进 USB Blockchain 作为对所有人开放的协议的应用前景。添加复杂性的优化将不会被接受，除非它们提供了非常根本性的益处。

2.通用原则 - 没有“特性”是 USB Blockchain 设计哲学中的一个根本性部分。取而代之的是，USB Blockchain 提供了一个内部的图灵完备的脚本语言以供用户来构建任何可以精确定义的智能合约或交易类型。想发明

你自己的金融衍生品？用 USB Blockchain，你可以。想创造你自己的货币？把它做成一个 USB Blockchain 合约就好。想建立一个全规模的守护程序（Daemon）或天网（Skynet）？你可能需要几千个联锁合约并且确定慷慨地喂养它们，一切皆有可能。

3.模块化原则 - USB Blockchain 的不同部分应被设计为尽可能模块化的和可分的。开发过程中，应该能够容易地让在协议某处做一个小改动的同时应用层却可以不加改动地继续正常运行。类似“短剑”（Dagger），“帕特里夏树”（Patricia trees） and“递归长度前缀编码“（RLP, recursive length prefix encoding,）等创新应该以独立的库的形式实施并且应该特性完整，以便于让其它的协议同样使用，即便 USB Blockchain 不需要其中的某些特性。USB Blockchain 开发应该最大程度地做好这些事情以助益于整个加密货币生态系统，而不仅是自身。

4.无歧视原则 - 协议不应主动地试图限制或阻碍特定的类目或用法，协议中的所有监管机制都应被设计为直接监管危害，不应试图反对特定的不受欢迎的应用。你甚至可以在 USB Blockchain 之上运行一个无限循环脚本，只要你愿意为其支付按计算步骤计算的交易费用。

5.基础区块创建-在内核中，USB Blockchain 的起点是一个相当规则的使用内存困难的工作量证明机制挖矿的不附带多少额外复杂度的加密货币，USB Blockchain 在许多方面比我们今天使用的基于比特币的加密货币简单。由多个输入输出构成的交易概念被更直观的基于平衡账目的模型取代了。序列号和锁定时间都取消了，并且所有的交易和区块数据都用单一格式编码。与比特币中对公钥加上 04 前缀后进行 SHA256 哈希再进行 RIPEMD160 哈希形成地址的方法不同，这里简单地取公钥的 SHA3 哈希的最后 20 字节作为地址。与其它致力于提供大量的“特性”的加密货币不同，USB Blockchain 致力于不提供特性，而是通过一个名为“合约”的涵盖所有的机制为用户提供近乎无限强大的功能。

2.5 USB Blockchain 客户端 P2P 协议

USB Blockchain 客户端 P2P 协议是一个相当标准的加密货币协议，并且能够容易地为其它加密货币使用；仅有的改动是引入了由 Yonatan

Sompolinsky 和 Aviv Zohar 在 2013 年 12 月首次引入的“幽灵“协议（"Greedy Heaviest Observed Subtree" (GHOST) protocol）；

该协议的引入动机和实现细节将在后面作详细介绍。USB Blockchain 客户端基本上是被动的；如果没有被触发，它自己做的仅有工作是调用网络守

护进程维护连接及定期发送消息索要以当前区块为父区块的区块。然而，该客户端同时会更强大；与只存储与块链相关的有限数据的 bitcoind 不同，USB Blockchain 客户端将同时扮演一个功能完整的区块浏览器的后台的角色。

当客户端收到一个消息时，它将执行以下布骤：

1.哈希该数据，并且检查该数据与其哈希是否已经接收过，如果是，退出，否则将数据发送给数据分析器。

2.确认数据类型。如果该数据项是一个交易，如果交易合法则将其加入本地交易列表，加入当前区块并发布至网络。如果该数据项是一个消息，作出回应。如果该数据项是一个区块，转入步骤 3。

3.检查区块中的“父区块“参数是否已存储于数据库中。如果没有，退出。

4.检查该区块头以及其“叔区块列表”中所有区块头中的工作量证明是否合法，如有任意一个非法，退出。

5.检查“叔区块列表”中每一个区块的区块头以确定其是否以该区块的“祖父区块”为父区块。如有任何否，退出。注意叔区块头并不必须在数据库中；他们只需有共同的父区块并有合法的工作量证明。

6.检查区块中的时间戳是否最后至未来 15 分钟并且在其父区块的时间戳之后。检查该区块的难度与区块号码匹配。如任何检查失败，退出。

7.由该区块的父区块的状态开始，加上该区块中的每一笔合法交易。最后，加上矿工奖励。如果结果状态树的根哈希与区块头中的状态根不匹配，退出。如匹配，将该区块加入数据库并前进至下一步。

8.为新区块确定 TD(block) ("总难度")。TD 由 TD(genesis_block) = 0 及 TD(B) = TD(B.parent) + sum(u.difficulty for u in B.uncles) + B.difficulty 递归定义。如新区块拥有比现区块更高的总难度，则新区块将成为“现区块“并进入下一步，否则，退出。

9.如果新区块被改动，向其中加入交易列表中的所有交易，废除交易列表中的所有变为不合法的交易，将该区块及这些交易向全网重新广播。

“现区块”是由矿工存储的一个指针；它指向矿工认为表达了最新的正式的网络状态的区块。所有索要平衡账目，合约状态等的消息都通过查询现区块并计算后回应。如果一个节点在挖矿，过程有一点轻微的改动；在做上述所有步骤的同时，该节点同时在现区块挖矿，将其自己收集的交易列表作为现节点的交易列表。

上述的“叔区块”应该是仅有的对比特币用户来说的新的概念；该思想来自于USB Blockchain对幽灵协议的独家的实施。幽灵协议提出的动机是当前快速确认的块链因为高作废率而受到低安全性困扰；因为区块需要花一定时间（设为 t）扩散至全网，如果矿工 A 挖出了一个区块然后矿工 B 碰巧在 A 的区块扩散至 B 之前挖出了另外一个区块，矿工 B 的区块就会作废并且没有对网络安全作出贡献。此外，这里还有中心化问题：如果 A 是一个拥有全网 30%算力的矿池而 B 拥有 10%的算力，A 将面临 70%的时间都在产生作废区块的风险而 B 在 90%的时间里都在产生作废区块。因此，如果作废率高，A 将简单地因为更高的算力份额而更有效率，综合这两个因素，区块产生速度快的块链很可能导致一个矿池拥有实际上能够控制挖矿过程的算力份额。

通过在计算哪条链“最长”的时候把废块也包含进来，幽灵协议解决了降低网络安全性的第一个问题；这就是说，不仅一个区块的父区块和更早的祖先块，该区块的父区块和更早祖先块的作废的兄弟区块也被加进来以计算哪一个区块拥有支持其的最大工作量证明。因为简洁性原则，USB Blockchain仅采用了幽灵协议的最基础部分（即废块必须以下一个区块的叔区块的身份纳入计算），但这已经获得了幽灵协议 90%以上的益处。另外，USB Blockchain付给以“叔区块”身份为新块确认作出贡献的废区块 75%的奖励（把它们纳入计算的“侄子区块”将获得奖励的 12.5%）；这个修改旨在解决第二个问题 - 中心化倾向。

2.6 USB Blockchain货币及其发行

USB Blockchain网络包含其内建的货币，咨询币，在网络内包含一种货币的原因是双重的。首先，咨询币被奖励给矿工以促进网络安全。其次，用它来支付交易费用是一种反欺诈机制。类似 Hashcash 的以交易为单位的工作量证明和放任自由是收取交易费的两个替代方案，前者浪费资源并且对于低档计算机和智能手机是一种不公平的折磨，后者将会导致网络立刻被无限

循环的“逻辑炸弹”合约淹没。咨询币有一个理论上的最大量 - 2128 单位(比照比特币的 250.9 单位)，虽然在可预见的将来不会有超过 2100 单位被发行。为方便和避免将来的争论（参见现在关于 mBTC/uBTC/聪的争论），这里提前为一些数额设定单位：

1：伟

103：(未定)

106：(未定)

109：(未定)

1012：萨博

1015:芬尼

1018：USB

这将是“元”和“分”或者“比特币”和“聪”的概念的扩展版，旨在成为将来的证据；看起来只有萨博，芬尼和 USB 会在可预见的将来被使用。“USB”将成为系统的主单位，很像元或比特币。为 103，106 和 109 命名的权力保留，未来将经过我们预批准后作为高级的辅助奖励授予投资者。

发行模型如下：

例如：咨询币将以每咨询币 0.0001 比特币的价格发售给投资者。假设此方式售出 X 咨询币。

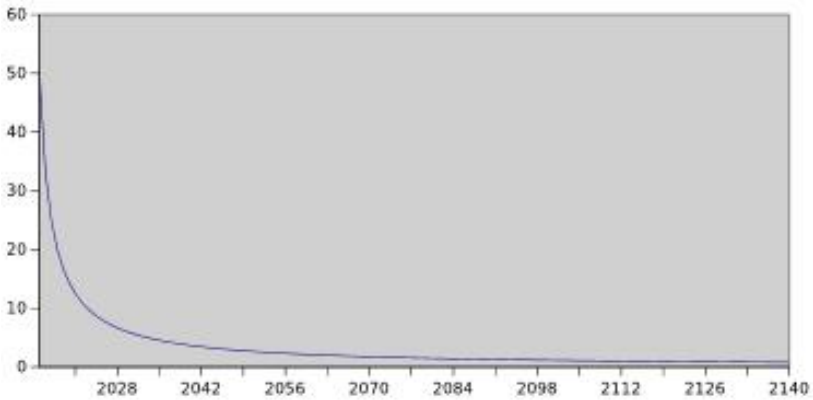
0.25X 咨询币将依照时间锁定合约分配给创业团队，一年内不得花费。

0.25X 将分配给 USB Blockchain 组织的预留资金池，以用来以工资或悬赏的形式支付给那些愿意部分或全部接受咨询币的开发者。

每年都将有 0.5X 咨询币将被矿工挖出。

	1 年后	5 年后
货币单位	2X	4X
投资者	50%	25%
创建者	12.5%	6.25%
预留	12.5%	6.25%
矿工	25%	62.5%

长期通胀率（百分比）



正如比特币选择一种长期来看通胀率趋近于零的发行方式，我们也放弃线性增长的发行方式

举例来说，假设五年内没有发生交易，25%的咨询币将会在投资者手里，6.25%属于创业团队，6.25%属于预留池，还有 62.5%属于矿工。永久线性通胀模型降低了在比特币那里看到的财富过度集中的风险，并且给予了生活在现在和将来的个人公平的获取财富的机会，同时能够激励人们获取和持有咨询币，因为从长远来看通胀率依然是趋近于零的（例如在第 1000001 年货币供应会从 500001.5 * X 上升到 500002 * X，通胀率 0.0001%）。此外，很多对于 USB Blockchain 的兴趣是中期的。我们预测如果 USB Blockchain 成功则它在 1-10 年的时间段内会经历巨大的增长，而在这期间它的供应量是非常有限的。

2.7 USB Blockchain 数据格式

USB Blockchain 中的所有数据都以“递归长度前缀编码（recursive length prefix encoding,RLP）”形式存储，这种编码格式将任意长度和维度的字符串构成的数组串接成字符串。例如，['dog', 'cat']被串接（以字节数组格式）为 [130, 67, 100, 111, 103, 67, 99, 97, 116]；

其基本的思想是把数据类型和长度编码成一个单独的字节放在实际数据的前面（例如‘dog’的字节数组编码为[100, 111, 103]，于是串接后就成了[67, 100, 111, 103].）注意 RLP 编码正如其名字表示的一样，是递归的；当 RLP 编码一个数组时，实际上是在对每一个元素的 RLP 编码级联成的字符串编码。需要进一步提请注意的是，USB Blockchain 中所有数据都是整数；所以，如果有任何的以一个或多个 0 字节开头的哈希或者地址，这些 0 字节应该在计算出现问题的时候去除。USB Blockchain 中没有串接数据结构包含任何以 0 开头的数值。整数以大端基础 256 格式存储（例如 32767 字节数组格式为[127, 255]）。

一个完整的区块的结构是：

```
[

block_header, transaction_list, uncle_list
]

Where:

transaction_list = [ transaction 1, transaction 2,
...
```

]

uncle list = [uncle_block_header_1, uncle_block_header_2,
...

]

block_header = [parent hash,

sha3(rlp_encode(uncle_list)), coinbase address, state_root,

sha3(rlp_encode(transaction_list)), difficulty,

timestamp, extra_data, nonce
]

每个 transaction 和 uncle_block_header 都是一张表。工作量证明数据是区块数据去除掉 nonce（交易数）后的 RLP 编码。

uncle_list 和 transaction_list 分别是叔区块头和区块里的交易构成的表。nonce 和 extra_data 都被限制为最大 32 字节，除了在

创世区块中参数 extra_data 会更大。

state_root 是一个包含所有地址的（key, value）对的默克尔-帕特里夏树（Merkle Patricia tree ）的根， 其中每一个地址都由一个 20 字节二进制字符串表示。对于每个地址，储存在默克尔-帕特里夏树的 value 字段是一个对以下格式对象进行 RLP 串接编码形成的字符串：

[balance, nonce, contract_root]

nonce 是该地址的交易数，每做一次交易都会增加 1。其目的是(1)使每个交易只有一次合法的机会以防范重放攻击，(2)使得构建一个和已存合约有相同哈希的合约成为不可能（更准确地说，密码学意义上不可行）。balance 指的是合约或地址的平衡账目，以伟为单位。contract_root 是另一个帕特里夏树的根，在该地址被一个合约控制的情况下包含该合约的内存。如果一个地址没有被一个合约控制，contract_root 就会是一个空字符串。注意在主帕特里夏树中所有地址的长度都是 20 字节，即便它们以一个

或多个 0 字节开头，在合约子树中所有索引都具有 32 字节的长度，如果不够长则加 0 前缀补足。

挖矿算法

基于过去五年比特币和替代币的经验，发现的一个对于工作量证明功能很重要的特性是“内存困难”-合法的工作量证明不仅需要大量的计算，同时需要大量的内存。如今，存在两个主要的“内存困难”功能类别 - scrypt 和质数币挖矿，但二者都不完美；没有一个需要理想的内存困难功能可能需要的内存，二者都会遭受时间-内存置换攻击，攻击中攻击者可以以牺牲一些计算效率为代价以远低于算法要求的内存大小完成合法工作量证明。USB Blockchain 使用一个替代的名为“短剑”（Dagger）的算法，一个基于适度直连的无环图的内存困难的工作量证明机制，它虽然远非最佳，但却有远较现存其它算法为强的内存困难特性：根据参数选择，每线程估计需要 50-500MB 的 RAM.

2.8 USB Blockchain 交易实现

一笔交易的数据结构是:

[nonce, receiving_address, value, [data item 0, data item 1 ... data item n], v, r, s]

nonce 是该地址已经发送的交易数量，编码为二进制格式(例如 0 -> '', 7 -> '\x07', 1000 -> '\x03\xd8'). (v,r,s)是新生成的不含用发送地址对应的私钥签名的 Electrum 风格的交易签名，v 的范围是 27 <= v <= 30. 从一个 Electrum 风格的签名(65 字节)可以直接提取出公钥和地址。交易合法的条件： (i)签名具有合法格式 (即 27 <= v <= 30, 0 <= r < P, 0 <= s < N)，以及 (ii) 发送地址具有足够的资金支付交易金额和交易费用。 一个区块不能够包含一个非法的交易；如果一个合约产生了一个非法交易则该交易将直接无效。交易费用将被自动包含。如果一个用户自愿支付更高费用，他总可以通过构建一个合约来自动地发送一定数量或一定比例的金额给现区块的矿工同时加速交易确认。

发送给空地址的交易是一种特殊类型的交易，创建了一个“合约”。

难度调整

难度根据下面的公式调整：

D(genesis_block) = 2^36 D(block) =

if anc(block,1).timestamp >= anc(block,501).timestamp + 60 * 500: D(block.parent) - floor(D(block.parent) / 1000)

else: D(block.parent) + floor(D(block.parent) / 1000)

anc(block,n) 是该区块（block）的第 n 代祖先；所有创世区块之前的区块都被假定为拥有和创世区块一样的时间戳。这会自动地把产生一个区块的时间稳定在 60 秒左右。选择 500 是考虑到过小的值会导致拥有足够算力的经常挖出两个连续区块的矿工修改时间戳以获取最大收益，而过大的值会导致难度震荡得过于剧烈，当选取常数 500，，模拟显示全网算力固定的情况下难度变化幅度是+/-20%。

第三部分 USB Blockchain 运营架构

3.1 USB Blockchain 主体：SAXSON 资本集团

USB Blockchain 运营团队来自 SAXSON 资本集团，一家历史悠久与备受推崇的美国上市公司(股票代码：SCGX)，财富管理行业的先驱，拥有了超过 30 年的财富管理专才。遍布全球拥有多个办事处，SAXSON 资本集团处于特别有利的地位为亚洲投资者提供全方位的财富管理咨询服务。

成立于 1983 年，SAXSON 资本集团的服务领域包括财富管理、基金投资、另类投资与金融咨询方案等。通过全球化的战略合作伙伴和精英化的服务团队，身处世界各地金融市场最前线的位置时刻掌握最新金融资讯，SAXSON 资本集团为投资者提供最有效的投资理财方案与金融咨询服务。SAXSON 资本集团，是私募股权基金的业界先驱之一，持有澳大利亚金融管理局颁发的“AFSL”金融牌照。

集团在全球 10 个办事处招募了超过 580 名专业人士，多元化的 12 只基金管理着超 250 亿美元的资产。

Joey 博士是 SAXSON 资本集团的创始人，2017 年亲自出任首席执行官 CEO。在创办 SAXSON 资本集团前，Joey 博士就职于一家全球领先的投资银行为执行董事，负责公司财务，资金管理的监督，并为多家大型跨国公司提供并购建议。

他在推出综合基金，资金监管，各类资金的管理，以及集体投资管理的专业知识，再加上他的远见带领着公司茁壮成长。Joey 博士目前负责集团所有的投资程序，公司的投资策略，和所有新产品的开发与推出。

3.2 USB Blockchain 基金会的设立

由 SAXSON 资本集团发起的 USB Blockchain 基金会（以下简称“基金会”）是 2016 年 11 月正式在美国成立的非营利性公司。USB Blockchain 基金会致力于 USB Blockchain 的开发建设和治理透明度倡导及推进工作，促进开源生态社会的安全、和谐发展。

多次采取硬分叉的解决方式使得人们对以太坊、乃至区块链的去中心化理念产生质疑。为避免客户端出现交易不一致，或者其他有违区块链设计理念的事件再次出现，USB Blockchain 基金会将通过制定良好的治理结构，帮助管理开源社区项目的一般轶事和特权事项。

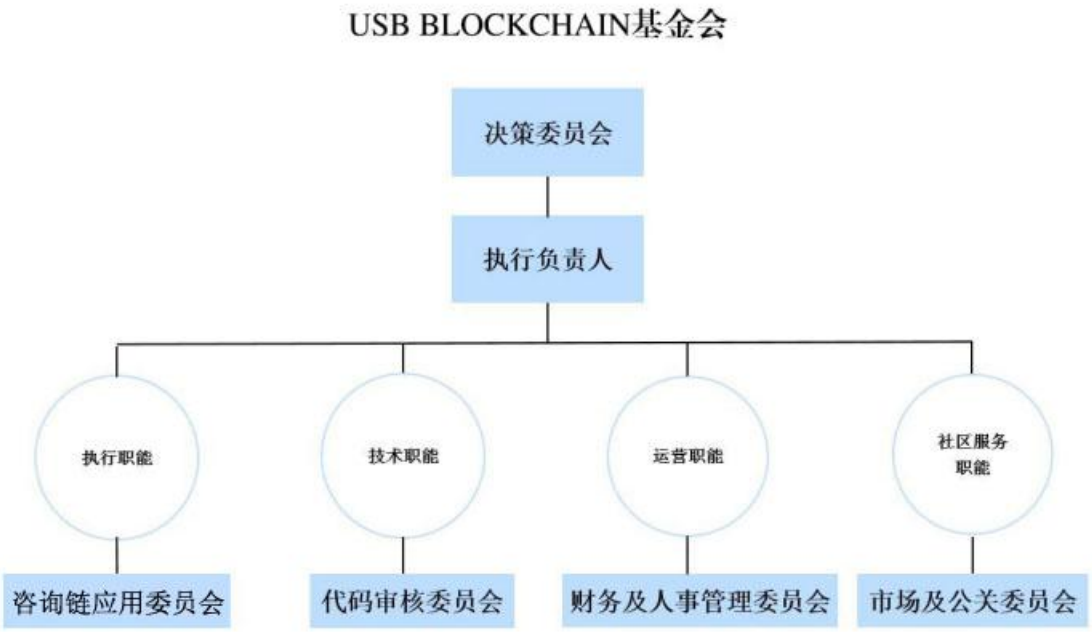
USB Blockchain 基金会治理结构的设计目标主要考虑开源社区项目的可持续性、管理有效性及募集资金的安全性。基金会由开发人员和职能委员会组成，组织架构主要由决策委员会、代码审核委员会、财务及人事管理委员会和市场及公共关系委员会组成。基金会成立初期，决策委员会由基金会主

席 Joey 博士、USB Blockchain 核心开发人员和私募成员组成，每期任期为二年。

3.3USB Blockchain 基金会管理架构

USB Blockchain 基金会治理架构包含了针对日常工作和特殊情况的操作流程和规则。本节将详细介绍基金会各职能委员会的职责。

USB Blockchain 基金会组织架构包括（如下图）：



决策委员会

USB Blockchain 基金会设立决策委员会，其职能包括聘任或解聘执行负责人以及各职能委员会负责人、制定重要决策、召开紧急会议等。决策委员会成员和基金会主席任期为两年，基金会主席不可连任。

首届 USB Blockchain 基金会决策委员会成员在区块链领域中具有丰富的行业经验，简要经历如下：

首席执行官 (CEO)	Joey 博士	Mr. Joey
首席运营官 (COO)	哈里·彼得·克拉克博士	Dr. Harry Peter Clarke
首席投资官 (CIO)	安东尼 - 帕克先生	Mr. Anthony Parker
运营经理	帕特里克·奥康纳先生	Mr. Patrick O'Conner
投资经理	罗杰·扬先生	Mr. Roger Young
法务经理	斯泰西·德席尔瓦博士	Dr. Stacy de Silva
货币经理 - 欧元流动	黛布拉·赖兰女士	Ms. Debra Rylands
基金经理 - 环球高收益	爱德华·马丁斯先生	Mr. Edward Martins
客户经理 - 金砖四国	刘英明先生	Mr. Samuel Liu
基金经理 - 环球近取股票	布莱恩·柯林斯先生	Mr. Brian Collins
基金经理 - 日本优势	川井小泽先生	Mr. Kenji Ozawa
营销经理 - 新兴市场股债优势	哪基胡森先生	Mr. Najeeb Hasan
股票经理 - 新领域股票	大卫·布朗尼先生	Mr. David Brownie
基金经理 - 环球股债收息	克里斯蒂娜·多纳多尼博士	Dr. Christina Donadoni
战略顾问 - 战略增长基金	伊恩·阿尔伯特·皮克林先生	Mr. Ian Albert Pickering

决策委员会任期期满后由社区根据咨询币币数和币龄计算权重进行投票选出 50 名社区代表，再进行投票选出 11 位决策委员会的核心人员，被选出的核心人员将代表USB Blockchain基金会做重要和紧急决策，并需在任职期间接受授信调查，并公开薪酬情况。

凡下列事项，需经过决策委员会以记名的投票方式进行表决，每名决策委员会成员有一票投票权，基金会主席有两票投票权。决策委员会做出决议，必须获得全体在任委员会成员的过半数通过：

修改基金会治理架构；

任免执行负责人及各职能委员会负责人；

制定重要决策；

决策委员会成员在任期内的任免，如成员违反职能范围、法律、行政法规、主动辞职等

紧急事件，如影响整个社区的事件、软件安全、USB Blockchain 系统升级等

此外，当有下列情况之一时，执行负责人应在 5 个工作日之内召集决策委员会举行临时会议：

基金会主席认为必要时；

三分之一以上决策委员会成员联合提议时；

执行负责人提议时

决策委员会会议应由委员会成员本人出席。因故不能出席的，可以书面委托委员会其他委员代表出席。未委托代表的，视为放弃在该次会议上的投票权。

执行负责人

执行负责人由决策委员会选举产生，负责基金会的日常运营管理、各下属委员会的工作协调、主持决策委员会会议等。执行负责人定期向决策委员会汇报工作情况。

USB Blockchain 应用委员会

USB Blockchain 应用委员会负责筛选适合的行业，将 USB Blockchain 技术应用到行业中，从而实现商业落地。

代码审核委员会

代码审核委员会由 USB Blockchain 开发团队中的核心开发人员组成，负责底层技术开发、开放端口开发和审核、各产品开发和审核等。此外，各产品的开发人员每周召开项目追踪会议，沟通项目进展及需求。代码委员会成员每日了解社区动态和热点，在社区中与 Token 持有者进行沟通交流，并且不定期举办技术交流会。

财务及人事管理委员会

财务及人事管理委员会负责项目募集资金的运用和审核、开发人员薪酬管理、日常运营费用审核等；目前日常的账务处理暂时外包给第三方。

市场及公共关系委员会

市场及公共关系委员会的目标是为社区服务，负责USB Blockchain技术推广、USB Blockchain产品推广、开源项目的推广和宣传等。此外，委员会还负责对外公告管理。若发生影响基金会声誉的事件，经内部审核评估后，统一由委员会进行公关回应。

3.4 USB Blockchain团队

USB Blockchain拥有一个非常有经验国际化团队，团队成员具有多年的区块链行业、密码学和虚拟货币社区的经验。USB Blockchain项目开发团队共有 10位核心开发者，由以太坊核心技术团队成员组成带领，完成 USB Blockchain 原型的开发。USB Blockchain主要团队成员及经历如下：

姓名	简要经历
Neson	拥有 ISCAE 的工商管理硕士，后来专攻计算机科学领域，拥有超过 20 年计算机科学与应用经验。
Joe chou	十三岁开始编程，目前已经审核过超过 100 种数字货币的设计，并发现若干安全漏洞，是数字货币社区中值得信赖的知名成员。
Chial	Chial 是一名经验丰富的 web 开发者，曾就职于百度任技术高管。
Mike wong	Mike 是区块链开发者、爱好者，2013 年投身于区块链行业，并参与多个加密货币项目的开发工作。
Adent	拥有 C、C++、Qt、QML 开发领域超过 9 年的经验，致力于跨平台应用的开发。在区块链开发超过一年的经验。
Alex	Alex 是大数据、区块链技术和系统安全的全栈开发人员。Alex 曾参与了 blockverify 和 OmniBazaar 等项目。
Millie Froncy	Brett 曾在 1999 年至 2004 年担任 Linux 系统管理员工作，2005-2014 年就职于 2013 年年中，开始进入区块链行业至今，有多年操盘区块链经济的经验，2017 年加入了USB Blockchain 大家庭。
Roman	Roman 是一名高级全栈开发人员，在构建分布式区块链解决方案方面拥有超过 3 年的经验。此外，他还是比特币、以太坊和智能合约方面的专家。
John	John 从 2012 年开始关注比特币，并于 2013 年加入了比特币社区。John 曾是以太坊技术团队的核心成员，拥有多年的区块链经济架构设计经验。

3.5USB Blockchain 基金会人力资源管理

USB Blockchain 致力于打造全球最具影响力的咨询行业区块链经济，为确保技术层面的开发顺利和基金会运营持续有效，有别于传统企业和其他非盈利组织的人员招聘过程，基金会将招聘最顶尖的开发人员和管理人才。

人员招聘

招聘人员按照“竞争、择优、经验”的原则，进行两人以上的面试、背景调查（如工作履历、商业利益等）、录用审批、试用期制度等。

基金会部分管理职能如财务、法务、税务等将采用外包形式，需经过基金会财务及人事管理委员会和基金会主席同意，签订人力资源外包服务协议。

USB Blockchain 作为开源社区，不仅招聘专职开发人员，还会聘请业界知名的技术顾问，相关的聘请和薪酬支付均需要经过决策委员会、基金会代码管理委员会和财务及人事管理委员会审批，并签订合作条款。

绩效考核

决策委员会人员每年进行绩效考核，主要内容包括基金会资金运营、基金会管理情况和社区协调工作等，每年进行尽职调查并采取轮岗制，由社区投票结果选取下一届决策委员会成员，连任不得超过 3 届。

由于基金会开发人员来自不同国家，开发人员分为全职和兼职，因此基金会制定了薪酬管理和绩效考核制度的政策。开发人员需定期报告自己的工作进度及交流开发进程，由代码管理委员会对其进行绩效考核。此外，每年将持续进行尽职调查。

3.6 USB Blockchain 基金会的风险评估及决策机制

USB Blockchain 基金会为制定和完善风险管理体系和制度，要求每年就 USB Blockchain 可持续性进行安全评估，评估内容包括项目质量、项目进度、项目应用，例如智能合约和简单合约应用、威胁识别分析，管控措施评估分析，风险界定、处置等阶段。

基金会将根据事件特性，例如事件影响程度、影响范围、影响代币量和发生的概率进行分级，按照优先级进行决策，对于优先级高的事件，尽快组织基金会相关委员会进行决策。事件类型主要分为管理类事务和代码类事务：

对于基金会普通管理类事务，由基金会成员进行会议商讨，最终由财务及人事管理委员会和基金会主席共同决定。

对于开源社区的代码问题和筹集资金的使用问题，决策通常采取成员投票机制。社区中每个成员根据所持咨询币的数量和币龄绝对投票权重，通过基金会投票系统进行投票，投票结果将有导向性作用。决策委员会具有决定权，而社区投票结果将作为参考。

对于紧急事件（例如影响整个社区的事件、软件安全，系统升级等）的决策，由代码审核委员会审核后提交至决策委员会，决策委员会通过投票表决，采取特权机制落实到社区中。基金会将通过投票机制避免分歧的产生，若产生分歧，由决策层人员的咨询币数量和币龄决定投票权重。

3.7 USB Blockchain 基金会日常运营机制

USB Blockchain 基金会日常运营主要分为代码管理、财务管理、人力资源、市场推广及法务事项。基金会将通过以下各项控制活动对日常运营进行管理，但各项控制活动不仅限于此：

控制目标	控制活动	控制所有人
代码管理		
开源代码管理	底层架构代码为开源代码，存放在Github，由核心开发小组成员拥有修改审批权限。	代码审核委员会
源代码修改	提交人修改源代码，由核心开发小组审批后完成修改。	代码审核委员会
代码开发及修改	代码开发及修改人员需经过核心开发小组审批，授予权限后进行开发及修改。	代码审核委员会
代码测试	代码编写或修改后需要经过测试并汇总测试结果，确保测试结果无异常。	代码审核委员会
代码审核	代码由专人审核，通过自动或者人工方式审核代码，验证无误后在社区发布公告。	代码审核委员会
代码上线	代码上线之前由代码核心开发人员审核。	代码审核委员会
漏洞修复	当代码出现漏洞时，由开发人员进行修复和测试，经过代码审核委员会审批后	代码审核委员会

	上线。	
应急演练	定期和不定期对代码的开发环境和测试环境进行应急演练，由代码审核委员会负责计划和实施。	代码审核委员会
代码修改权限	对于非公开的产品代码，由代码审核委员会授予修改代码的权限，申请审批后方可操作。	代码审核委员会

控制目标	控制活动	控制所有人
人力资源		
招聘	招聘人员需经过两人或以上人员面试，经过独立评价后形成招聘记录。最终由相关委员会进行审批。	财务及人事管理委员会
背景调查（尽职调查）	对关键开发人员和关键岗位的招聘，需要经过尽职调查后方可录用，并留存调查文档。	决策委员会
专业服务外包	专业服务（财务、法务、税务等）外包经过财务及人事管理委员会评估审核后选定服务方，并签订外包协议。	财务及人事管理委员会
工资薪酬	决策委员会人员的工资薪酬应当披露；核心开发人员和管理人员的工资薪酬应当由决策委员会成员审核；其他人员工资薪酬应经过各委员会审核。	决策委员会
市场推广		
推广渠道的新增	由 PR 委员会对新增推广渠道进行调研，包括渠道的方向、可延伸性和推广力度。经过调研后审批确定新增的推广渠道。	市场及公共关系委员会
推广服务合同签订	新增推广服务或者渠道，需要经过 PR 委员会审批后签订合作协议。	市场及公共关系委员会
推广文案的编写及审核	推广文案需要经过独立人员审核后方可发布。	市场及公共关系委员会
危机公关处理	当出现紧急事件，需要有 PR 委员会商讨公关处理，由决策委员会同意后方可对外披露。	市场及公共关系委员会
财务管理		
预算审核	每年制定基金会运营预算，由财务负责人审核。	财务及人事管理委员会
合同的拟定与审核	由独立法务人员对合同条款进行审核。	财务及人事管理委员会
合同的签订	合同条款经过审核后，由决策委员会审核，审核后方可签订合同。	决策委员会
收入审核	基金会的收入来源主要是私募和咨询币	财务及人事管理委员会

	公开售卖，由财务人员进行核准并记录，由独立人员进行对账。	
支出审核	基金会所有支出需经过财务及人事管理委员会审核，并做好相关账务处理。	财务及人事管理委员会
账务处理	账务处理应由财务及人事管理委员会负责人审核，并且每月形成财务报告。	财务及人事管理委员会
资金对账	实物资金与资金账每月应当进行对账，由基金会财务及人事管理委员会授权人	财务及人事管理委员会

控制目标	控制活动	控制所有人
	员审核。	
披露事项	定期披露基金会募集的资金如何使用，基金会的发展情况应定期向社区汇报。披露事项需经过决策委员会审批。	决策委员会
合作外包条款的签订	基金会部分职能外包，由财务及人事管理委员会的审批后签订外包协议。	财务及人事管理委员会

USB Blockchain 基金会每年会接受外部机构对基金会募集资金的使用情况、利润、成本和潜在债务等进行评估和审计。

3.8 USB Blockchain 基金会的经济

USB Blockchain 基金会的财务管理团队分为日常财务管理和数字货币的管理。日常财务管理将外包，包括开发人员的差旅费、人员工资、房屋租赁、日常费用等；数字资产的管理由决策委员会授权人员负责，包括钱包管理、数字资产的到账、与其他数字货币的兑换、数字货币的兑现等。

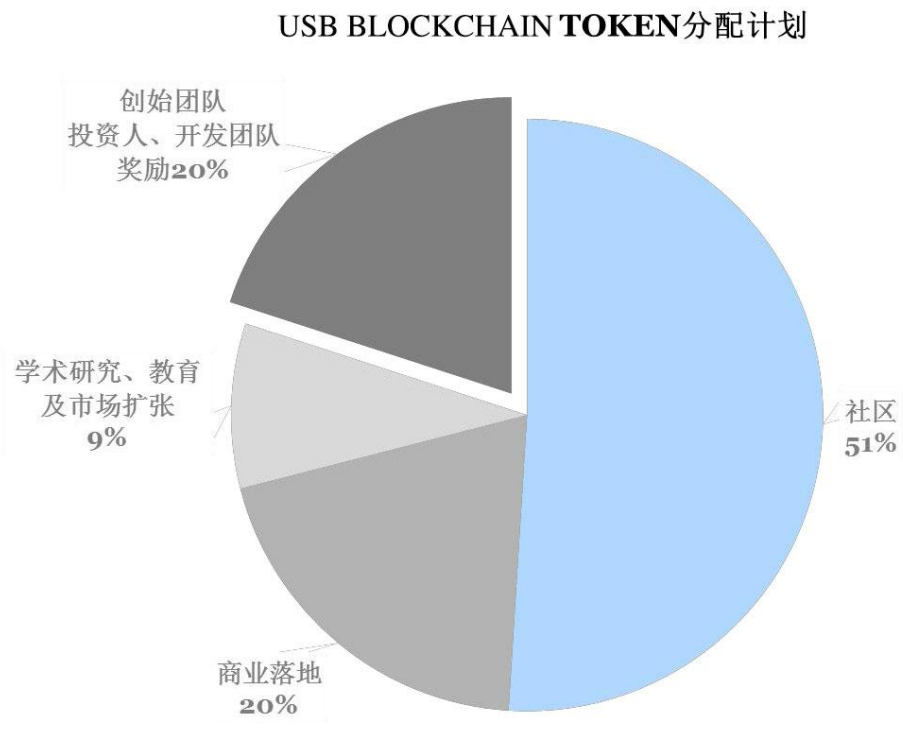
资金来源

USB Blockchain 基金会在开发初期不会产生大量收入，主要收入来自于私募和咨询币公开售卖，参与者需要使用咨询币获取 USB Blockchain 和 DApp 的使用权。

咨询币分配计划

咨询币的分配计划如下：最终 51%的咨询币将分发给社区，20%分配给创始团队、私募投资者和开发团队（详见图一）。

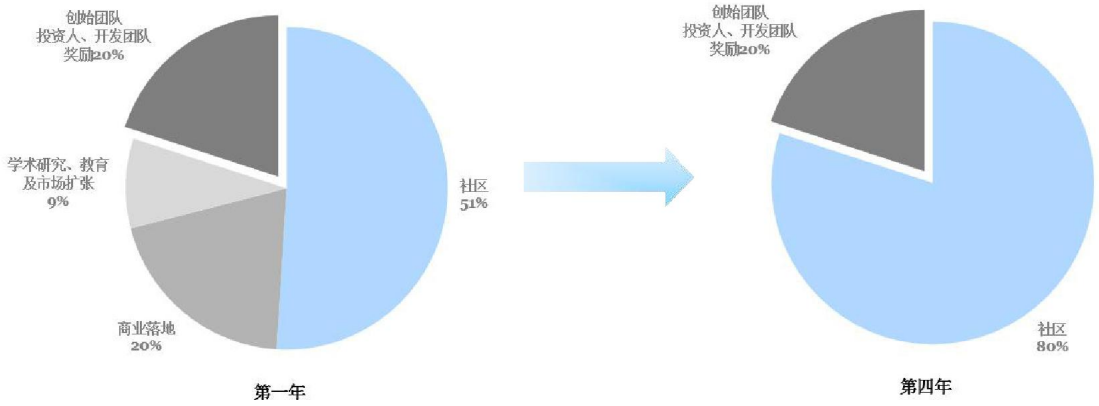
比例	分配方案	明细
51%	咨询币公开售卖	咨询币公开售卖获得的收入将会用于USB Blockchain基金 会的运营，包括开发、市场、财务和法律咨询等。
20%	创始团队、私募投资人和开发团队	创始团队、私募投资人以及开发团队在USB Blockchain的 发展过程中做出了人力、资源、物力以及技术的贡献，因此以发放咨询币作为回报。
20%	商业落地部署	筛选合适的行业，进行行业中的战略部署、项目扶持和代币置换，用于USB Blockchain技术的行业应用， 真正实现商业落地。
9%	学术研究、教育及市场扩张	用于支持USB Blockchain相关的学术研究、开发人员的教 育材料、提高对USB Blockchain技术的意识以及向其他开 源社区进行贡献。



第一年

图一

基金会计划将 29%（商业落地 20%；学术研究、教育及市场扩张 9%）分阶段逐步分配给社区，在三到四年后最终全部咨询币投放于社区（详见图二），使 USB Blockchain 真正实现开源的社区生态。这部分咨询币的运用将每年向社区公布并提供财务报告。



图二

比例	用途	钱包地址
10%	商业应用	待公布
10%	代币兑换	待公布
9%	学术研究、教育及市场扩张	待公布

资金使用的限制条款

咨询币的使用本着公开透明的原则，根据上述分配原则和钱包地址进行使用，由托管机构监督数字资产的流向并定期分享给社区。

公开售卖收入的使用原则：

超过 500 个 ETH，需要经过财务及人事管理委员会审批；

超过 1000 个 ETH，需要经过决策委员会审批。

财务规划和执行的报告

每季度由财务及人事管理委员会制定财务规划并对上一季度的财务执行情况进行总结，形成财务报告提交至决策委员会审核。

数字资产管理

属于 USB Blockchain 基金会的数字资产由财务及人事管理委员会授权人员负责，每天做交易记录，采取多重签名确保资产的安全性和准确性。所有收取的法币，及时转为数字货币，并存入数字钱包。基金会资产不得存于个人账户。

数字钱包管理

基于独立性原则，USB Blockchain 基金会的钱包采取 3/4 多重签名。若增加签名，须经过财务及人事管理委员会。大额的代币进行冷存储；小额的代币使用多重签名的方式。

咨询币的发行及管理

USB Blockchain 对应的咨询币是 USB Blockchain 和 DApp 的使用权。初次发行总量的 51%，总量固定 10 亿枚。

披露事项

每年基金会将向社区披露 USB Blockchain 的开发情况、公链的运营情况、咨询币的使用情况以及基金会的运作是否符合治理章程。

3.9 其他事项及法律事务

法律事务

USB Blockchain 基金会在美国成立，若出现需要寻求法律意见的事项，需要通过当地律师予以确认。

免责条款

USB Blockchain 基金会目标转变为非营利组织，链上用户获取的是 USB Blockchain 的使用权。购买者应明白

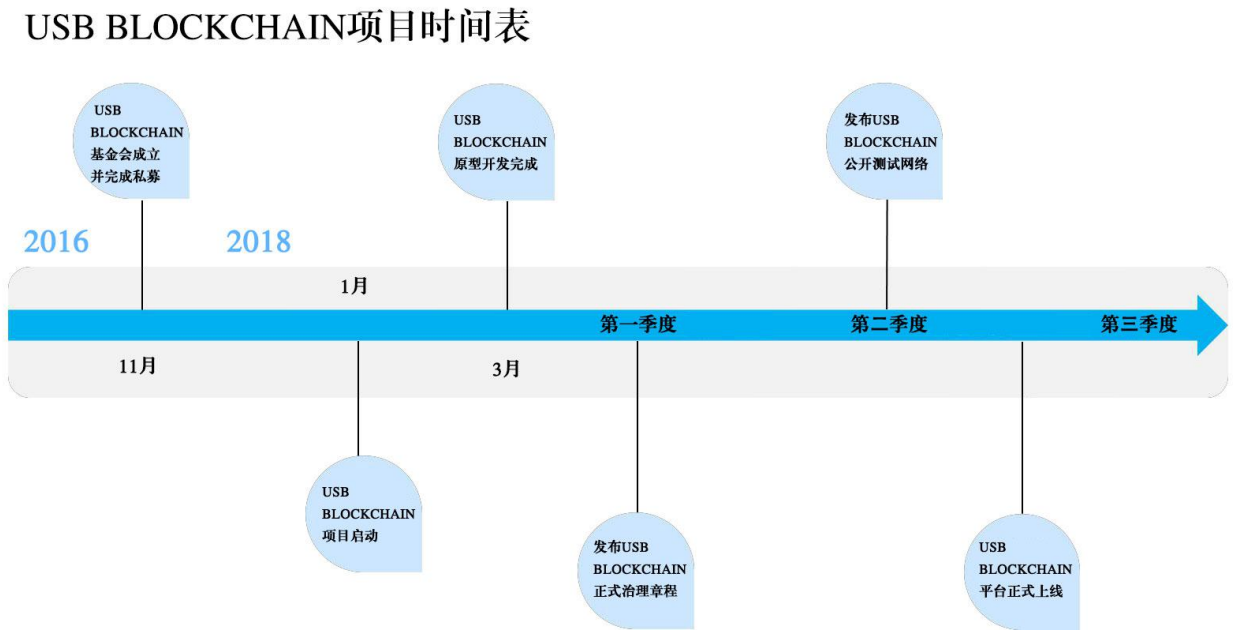
在法律范围内，咨询币不做任何明示或暗示的保证，并且咨询币是“按现状”购买的。此外，购买者应明白咨询币不会在任何情况下提供退款。

争议解决条款

当出现争议时，有关方面应依据协议通过协商解决。如协商解决无法解决，可通过法律解决。

第四部分 USB Blockchain 实施及迭代

4.1 USB Blockchain 上线的时间规划



USB Blockchain 项目的主要时间节点包括:

USB Blockchain 项目启动：2018 年 1 月联合创始人正式启动 USB Blockchain 项目;

USB Blockchain 原型开发完成：2018 年 3 月，开发团队完成了 USB Blockchain 原型的开发;

由 SAXSON 资本集团发起的基金会成立并完成私募：USB Blockchain 基金会于 2016 年 11 月在美国成立了非营利性公司，并得到了数百万美金的种子轮投资，部分投资人以太坊早期参与者 Anthony Di Iorio、OKCoin CEO 、BitFund 创始人等参与。

公开售卖计划公布：公布公开售卖计划，包括售卖目标、售卖期间、售卖方式和奖励等;

咨询币公开售卖：根据公布的公开售卖计划，通过合作渠道进行公开售卖；

4.2 USB Blockchain 项目公开售卖计划

USB Blockchain 的用户需通过消耗持有的咨询币来获取 USB Blockchain 的功能，尤其在 USB Blockchain 上运行分布式应用需要支付和消耗一定量的咨询币。

咨询币将会在 USB Blockchain 正式发布时全部产生，由 USB Blockchain 基金会持有。

咨询币公开售卖的具体规则和信息将会通过 USB Blockchain 官网网站进行公布。

参与 USB Blockchain 售卖不是零风险的。详细内容，请参阅 PROSPECTUS 第五章“风险因素”。

募集对象的具体权利义务请参见 PROSPECTUS：Chapter III& Chapter IV。

4.3 USB Blockchain 的未来迭代规划

作为区块链技术，会面临各种挑战和机遇，USB Blockchain 的未来迭代包括两部分，一是代码本身的迭代；二是商业应用上的迭代。

USB Blockchain 底层架构的迭代

当 USB Blockchain 代码本身出现漏洞，通常采取系统升级。出现漏洞需要经过代码委员会进行分析、测试和审核，提交至决策委员会报备。当出现以下重大漏洞（不限于）采取系统升级：

影响用户资金

重大安全问题

影响系统安全

当出现较小的漏洞时，直接由代码委员会进行补丁。

商业应用上的迭代

USB Blockchain 将会是完全开源的项目，USB Blockchain 系统希望通过技术上的创新、理念上的创新将区块链与现实链接起来。因此在商业应用的时候，USB Blockchain 基金会会选择合适的第三方合作，进行行业和应用的迭代。由第三方供应商主导，USB Blockchain 提供相应技术支持。

第五部分 USB Blockchain 未来应用

5.1 去中心化应用

区块链技术的一大特点就是去中心化，而 USB Blockchain 系统致力从技术层面全面支持去中心化应用，USB Blockchain 开发不同模块，提供适用于不同系统和不同用户的开发平台，简化开发者的准备工作，从而实现快速开发。另外通过移动端策略的引入，将不同的 DApp 想法产品化，使普通互联网用户可以真正分享到区块链技术带来的价值。

面向不同行业的 DApp 应用，可以把区块链技术带给更多的用户和行业。例如去中心化的社交、去中心化的存储和去中心化的域名服务、去中心化的计算服务等，通过激励机制的引入，将更深层次利用共享经济的理念，改变现有的 APP 市场和商业模式。

5.2 中国咨询行业发展现状及前景分析

中国的体制转型将为咨询业创造出广阔的发展前景和市场潜力。在未来的 10 年中，中国咨询行业的需求将以每年 10 倍的速度增加，到 2020 年中国咨询行业的有效需求总额将达到 250 亿美元。这说明我国咨询业的前景非常广阔。然而任何一个行业的发展都不是一帆风顺、完美无缺的，在发展不成熟的阶段必然会面临一些问题。咨询行业是知识型产业，而这其中一项重要的问题就是，作为这一产业核心资源的专业技术人员根本不可能以相应的速度培养，专业技术人才成为巨大的一个缺口。而这就意味着 USB Blockchain 在中国的前景非常看好，并且拥有足够大的市场空间，在咨询行业，除去人才成本，最大的成本就是税务，而 USB Blockchain 则很好的解决了税务和交易问题，并且让交易变成资产，变成投资。

5.3 将颠覆全球所有咨询/资讯行业的支持与变革

在 USB Blockchain 系统中，通过引入支持行业共识机制和监管的需求，可以为行业发展需求也提供支持。

例如，USB Blockchain 系统可以满足可信网络中，对区块链速度和容量的要求，通过基于区块链技术的主控合约和 Oracle 和 Data Feeds 的引

入，也可以引入更多线下的因素。通过 Identity 和 Privacy 的设计，可以符合金融行业的监管需求。

在 USB Blockchain 系统中，可以支持多个咨询/咨询行业的应用需求：例如金融业、物联网、供应链、社交和游戏、慈善、数字资产和股权等。另外基于 USB Blockchain 的智能合约和主控合约，通过图灵完备的编程语言，可以实现更复杂商业逻辑的支持，并将支持更多的行业。

未来，所有的咨询行业都离不开 USB Blockchain，因为咨询币正在颠覆全球的咨询行业。

5.4 USB Blockchain 更适应当下的移动端策略

在 USB Blockchain 的生态系统中，我们不仅全面支持并推动移动应用战略，而且我们将会与第三方开发者，一起为用户提供移动端的服务，包括：移动端钱包、移动端 DApp 应用、移动端智能合约应用等服务。

USB Blockchain 开发团队计划建立 DApp Store，将区块链技术与现有的互联网产品和数字货币进行融合，例如微信、云计算等。USB Blockchain 已经发布的社区项目包括 BiSMTP 协议，宗旨是让每个 email 成为虚拟货币钱包。

5.5 USB Blockchain 的更多未来应用

1）储蓄钱包。假设 Alice 希望保障她的资金安全，但是担心自己货弄丢私钥或私钥被黑客盗走，那她可以把咨询币打进与 Bob（是一家银行）的合约里，规定如下：Alice 每天可以单独取款最多 1%的资金，Alice 和 Bob 一起可以取走全部，而 Bob 单独最多只能取 0.05%。通常一天 1%对于 Alice 是足够的，如果她想取更多可以找 Bob 帮忙；如果 Alice 的私钥被盗了，她可以赶紧跑去找 Bob 一起把资金转移到一个新的合约里；如果她丢了私钥，Bob 最终还是把资金（缓慢地）取出来的；如果最后发现 Bob 是恶人，那 Alice 可以以 20 倍 Bob 的速度把钱转走。

2）咨询服务保险。你可以很容易地建立金融衍生品合约，这里用的是行业的数据输入，而不是行业指数。如果一个衍生品合约支付出来的金额与咨询公司的排名相关，那么一个企业如果买它，就可以在排名下降的时候收

到补偿；而当排名上升的时候，他会很开心因为他的选择让自己的消费也变成更值得的投资。

3）一种以中心化方式管理的数据输入方式，它采用基于权益证明机制投票的最终结果的平均值（更可能是中位值）来代表人们对于某个数据的看法，这个数据可以是某种大宗商品的价格，或是其它相关数据。

4）多重签名智能契约。比特币允许基于多重签名的交易合约，例如，5把私钥里集齐 3 把就可以使用资金。USB Blockchain 可以做得更细化，例如，5 把私钥里集齐 4 把可以花全部资金，如果只有 3 把则每天最多花10%的资金，只有 2 把就只能每天花 0.5%的资金。另外，USB Blockchain里的多重签名是异步的，意思是说，双方可以在不同时间在区块链上注册签名，最后一个签名到位后就会自动发送交易。

5）点对点赌博。任意数量的点对点赌博协议都可以搬到 USB Blockchain 的区块链上，例如 Frank Stajano 和 Richard Clayton 的Cyberdice。最简单的赌博协议事实上是这样一个简单的合约，它用来赌下一个区块的哈稀值与猜测值之间的差额。之后，SatoshiDice 整个赌场都可以搬到区块链上去，这可以通过给每一次赌博创建一个合约来实现，也可以通过半中心化的合约来实现。

6）顺理成章，基于区块链的大规模股票市场，预测市场也很容易实施。

7）利用身份和信用体系，来实现一个基于区块链的去中心化市场。

8）去中心化的 Dropbox。先把文件加密，再建立它的 Merkle 树，然后把 Merkle 树的根和一定数量的咨询币一起根植到一个合约里，最后把文件散布到在某个次级网络上去。这个合约每天都会根据区块的哈稀值来随机选出 Merkle 树的一个分支，然后拿出一些咨询币给第一个为合约提供这个分支的节点，这个奖励就鼓励了节点们来长期存储数据。如果你想下载文件的任何一部分，你可以发送支付到某个提供微支付通道的合约，进而从多个节点下载文件，每个区块下载一部分。

第六部分 变革全球咨询行业的区块链应用场景

场景一：区块链技术应用于全球咨询行业的智能合约

Augur 是一个开源的、去中心化的预测市场平台，于 2015 年在以太坊上发布。Augur 使用了区块链技术执行智能合约。

在 Augur 平台上，任何一个人可以在任何地方都可以为自己感兴趣的主题（比如，2016 年美国大选谁会获胜）创建一个预测市场，不需要任何中心化的批准。作为回报，该市场的创建者将从市场中获得一般的交易费用。Augur 平台的另一个重要特性是可以减少诈骗和对手方风险：平台上的货币交易通过智能合约进行严格的监管，分布式 Oracle 系统可以确保没有人能对事件提出不真实的结果。

Augur 系统内部使用一种名为信誉（“REP”）的代币。当事件发生后，众多 REP 持有者对事件结果进行报告。而比特币和以太币用于市场的投资。

因此，Augur 使用分布式 Oracle 技术，允许智能合约在其上运行，建立了一个无需信任任何个人和组织的、高度自治可信的平台。

全球最大管理咨询公司麦肯锡咨询公司(McKinsey & Company)最近向美国联邦保险咨询委员会提交了一份区块链技术报告这份报告分析了区块链技术可能会如何颠覆广泛的行业，特别强调了银行和咨询业，同时报告还预测到 2021 年区块链技术会实现规模化商业部署。该公司表示该行业的大部分人都认为区块链技术将会在 3 到 5 年内产生“实质性影响”。

这 64 种不同的使用案例中有 24 个属于咨询类金融服务应用。然而，其中有 7 个被报告称为“真正的使用案例”，能够解决目前系统存在的一些“痛点”，并且指出这些案例将会带来最多的收入，同时也是最值得追求的使用案例。在这 7 种使用案例中，麦肯锡预计区块链将会产生了“800 到 1100 亿美元的收益”。

贸易金融：区块链能够降低成本和提高周转速度，可增加 140-170 亿美元的收入。

跨境 B2B 支付：区块链可以带来更低的成本和手续费，同时加快支付服务速度，将节约大约 500-600 亿美元。

跨境 P2P 支付：与 B2B 支付一样，区块链也可以降低该领域的成本同时加快速度，不过对于个人汇款，预计可以节约 30-50 以美元。

回购协议交易：区块链可以降低这种交易的成和系统性风险，预计价值大约 20-50 亿美元。

OTC 衍生品市场：区块链可简化结算流程，从而降低运营成本以及对资本的需要，预计可节约大约 40-70 亿美元。

KYC/AML 管理：区块链可减少重复工作以及疏通介入流程，预计可带来 40-80 亿美元收入。

身份欺诈：区块链带来更高的安全性，让消费者少受损失，预计可以节约 70-90 亿美元。

场景二：区块链技术应用于产品管理

在区块链上使用唯一的 ID，并将此 ID 与商品结合，通过跟踪商品，供应链中各方之间的沟通和合作以及政府机构的监督来创建一个透明的供应链，以解决与假冒产品有关的问题。

2016 年 11 月，一个基于区块链的产品管理平台 Vechain（“唯链”）发布。唯链可以为用户提供商品资产管理、追踪溯源、防伪校验和增强消费体验。通过在区块链上放置唯一 ID 并使用近场通信（“NFC”）芯片，射频识别（“RFID”）标签或快速响应（“QR”）代码嵌入每个产品，方便验证这些商品的真伪。 VeChain 为不同企业提供了一个轻松创建、管理、维护和更新共享数据的机会。

VeChain 还为在供应链上运行的各方的不同 IT 系统之间建立了连接。通过唯链的 APP，消费者可以直接查看所购商品在上游每个节点的信息，并能写入自己的数据。此外，唯链还能用于商品资产管理和用户体验等应用场景。

场景三：区块链技术应用于咨询行业的物业估值

区块链技术透过分布式分类账技术，建立及传送完整、加密的资料，有助提升资料的可追踪性，确保资料准确无误。

中国银行（香港）（“中银香港”）是香港主要上市商业银行集团之一，在 2016 年 11 月 28 日宣布正式推出物业估值区块链技术，并成功透过该技术与物业估价公司完成首宗物业估值。

区块链技术帮助银行精简验证估值报告流程，节省成本；物业估价公司也无需再提供纸质本的物业估值报告，有助推动无纸化绿色金融。

目前，中银香港与两家物业估值公司合作。为扩大区块链的应用，中银香港将邀请其他估值公司及银行同业参加，以丰富区块链内的物业估值资料。同时，香港金融管理局大力支持了此次物业估值区块链服务的推出。中银香港希望为金融科技在金融业应用带来更多创新概念和应用案例，令金融机构及消费者同时得益，促进银行界金融科技的发展。

除了物业估值按揭流程外，中银香港将继续积极探讨及研究，把区块链技术应用于其他领域，包括贸易融资、电子证件管理以及跨境支付等。

场景四：区块链将再造咨询行业游戏规则——五大应用场景解析

区块链“去中心化”的本质能让当今咨询行业交易所面临的一些关键性问题得到颠覆性的改变。根据麦肯锡分析，区块链技术影响最可能发生在支付及交易银行、资本市场及咨询类业务的主要应用场景。

以下分别针对数字货币、跨境支付与结算、票据与供应链金融业务、证券发行交易及客户征信与反诈欺等五大应用场景，探讨区块链技术将如何解决当前业务的痛点，以及科技金融公司正在实践哪些的区块链实用技术。

延伸场景一：数字货币：提高货币发行及使用的便利性

比特币的崛起颠覆了人类对货币的概念。比特币及其他数字货币的出现与扩展正在改变人类使用货币的方式。从过去人类使用实物交易，到发展物理货币及后来的信用货币，都是随着人类的商业行为及社会发展不断演进。随着电子金融及电子商务的崛起，数字货币安全、便利、低交易成本的独特性，更适合基于网络的商业行为，将来有可能取代物理货币的流通。

以比特币为代表的数字货币目前已在欧美国家获得相当程度的市场接受，不但能在商户用比特币支付商品，更是衍生出比特币的借记卡与 ATM 机等应用产品。数字货币与法定货币之间交换的交易平台也应运而生，例如美国最大的比特币交易平台 Coinbase 目前支持美金、欧元、英镑及加拿大币与比特币之间的兑换；中国的交易平台 OKCoin 及火币也支持人民币与比特币的交易；比特币与法定货币之间的庞大交易量与流动性足以被视为一种国际通行货币。正是比特币网络的崛起，让社会各界注意到其背后的分布式账本区块链技术，并逐渐在数字货币外的众多场景获得开发应用。

国家发行数字货币将成趋势。2015 年厄瓜多尔率先推出国家版数字货币，不但能减少发行成本及增加便利性，还能让偏远地区无法拥有银行资源的民众也能通过数字化平台，获得金融服务。突尼斯也根据区块链的技术发行国家版数字货币，除了让国民通过数字货币买卖商品，还能缴付水电费账单等，结合区块链分布式账本的概念，将交易纪录记载于区块链中，方便管理。

同时，其他许多国家也在探讨发行数字货币的可行性。目前，包括瑞典、澳大利亚及俄罗斯正在研讨发展数字货币的计划。英国央行正委托伦敦大学学院设计一套数字货币 RSCoin 进行试验，预期通过央行发行的数字货币来提高整体金融体系的安全性与效率。中国央行也在 2016 年 1 月召开数字货币研讨会，提出争取早日推出央行发行的数字货币。各国央行均认识到数字货币能够替代实物现金，降低传统纸币发行、流通的成本，提高支付结算的便利性；并增加经济交易透明度，减少洗钱、逃漏税等违法犯罪行为，提升央行对货币供给和货币流通的控制力；同时，通过发展数字货币背后的区块链技术应用，扩展到整个金融业及其他领域，确保资金和信息的安全，提升社会整体效能。

延伸场景二：跨境支付与结算：实现点到点交易，减少中间费用

当前的跨境支付结算时间长、费用高、又必须通过多重中间环节。拥有一个可信任的中介角色在现今的跨境交易非常重要，当跨境汇款与结算的方式日趋复杂，付款人与收款人之间所仰赖的第三方中介角色更显得极其重要。每一笔汇款所需的中间环节不但费时，而且需要支付大量的手续费，其成本和效率成为跨境汇款的瓶颈所在。如因每个国家的清算程序不同，可能导致一笔汇款需要 2 至 3 天才能到帐，效率极低，在途资金占用量极大。

区块链将可摒弃中转银行的角色，实现点到点快速且成本低廉的跨境支付。通过区块链的平台，不但可以绕过中转银行，减少中转费用，还因为区块链安全、透明、低风险的特性，提高了跨境汇款的安全性，以及加快结算与清算速度，大大提高资金利用率。未来，银行与银行之间可以不再通过第三方，而是通过区块链技术打造点对点的支付方式。省去第三方金融机构的中间环节，不但可以全天候支付、实时到账、提现简便及没有隐形成本，也有助于降低跨境电商资金风险及满足跨境电商对支付清算服务的及时性、便捷性需求。

延伸场景三：票据与供应链金融业务：减少人为介入，降低成本及操作风险

票据及供应链金融业务因人为介入多，导致许多违规事件及操作风险。从 2015 年年中，国内开始爆发票据业务的信用风暴。票据业务创造了大量流动性的同时，相关市场也滋生了大量违规操作或客户欺诈行为，陆续有多家商业银行的汇票业务事件集中爆发。国内现行的汇票业务仍有约 70%为纸质交易，操作环节处处需要人工，并且因为涉及较多中介参与，存在管控漏洞，违规交易的风险提高。供应链金融也因为高度依赖人工成本，在业务处理中有大量的审阅、验证各种交易单据及纸质文件的环节，不但花费大量的时间及人力，各个环节更是有人工操作失误的机会。要知道咨询行业最大的就是人工支出了！

延伸场景四：证券发行与交易：实现准实时资产转移，加速交易清算速度

证券的发行与交易的流程手续繁杂且效率低下。一般公司的证券发行，必须先找到一家券商，公司与证券发行中介机构签订委托募集合同，完成繁琐的申请流程后，才能寻求投资者认购。以美国的交易模式为例，证券一旦上市后，交易更是极为低效，证券交易日和交割日之间存在 3 天的时间间隔。

区块链技术使得金融交易市场的参与者享用平等的数据来源，让交易流程更加公开、透明、有效率。通过共享的网络系统参与证券交易，使得原本高度依赖中介的传统交易模式变为分散的平面网络交易模式。这种革命性交易模式在西方金融市场的实践中已经显现出三大优势：首先，能大幅度减少了证券交易成本，区块链技术的应用可使证券交易的流程更简洁、透明、快速，减少重复功能的 IT 系统，提高市场运转的效率。其次，区块链技术可准实时地记录交易者的身份、交易量等关键信息，有利于证券发行者更快速清晰地了解股权结构，提升商业决策效率；公开透明又可追踪的电子记录系统同时减少了暗箱操作、内幕交易的可能性，有利于证券发行者和监管部门维护市场。第三，区块链技术使得证券交易日和交割日时间间隔从 1-3 天缩短至 10 分钟，减少了交易的风险，提高了交易的效率和可控性。

延伸场景五：客户征信与反欺诈：降低法律合规成本，防止金融犯罪

银行的客户征信及法律合规的成本不断增加。过去几年各国商业银行为了满足日趋严格的监管要求，不断投入资源加强信用审核及客户征信，以提

升反欺诈、反洗钱抵御复杂金融衍生品过度交易导致的系统性风险的成效。2014 年，UBS 为了应对新的监管要求，增加了约 10 亿美元的支出；而汇丰集团在 2013 至 2015 年间，法律合规部门的员工人数从 2000 多人增至 7000 多名。为提高交易的安全性及符合法规要求，银行投入了相当的金钱与人力，已经成为极大的成本负担。

记载于区块链中的客户信息与交易纪录有助于银行识别异常交易并有效防止欺诈。区块链的技术特性可以改变现有的征信体系，在银行进行“认识你的客户”(KYC)时，将不良纪录客户的数据储存在区块链中。客户信息及交易记录不仅可以随时更新，同时，在客户信息保护法规的框架下，如果能实现客户信息和交易纪录的自动化加密关联共享，银行之间能省去许多 KYC 的重复工作。银行也可以通过分析和监测在共享的分布式帐本内客户交易行为的异常状态，及时发现并消除欺诈行为。

场景五：区块链技术应用于证券交易

2016 年 11 月 29 日，德国央行 Deutsche Bundesbank 无论从实力还是规模上都是欧洲央行体系（“ESCB”）最有影响力的成员，公开了区块链证券结算原型。

德国央行与德国证券交易所（“Deutsche Borse”）共同发起证券和股票交易市场原型，这是两家机构首个合作成果，只是改变原型，还不能实际推广。该产品为中央机构发行的数字货币和数字证券交易和转移提供结算技术支持，兼顾交易和支付流程；计划是两个月之后进一步开发原型，分析这种区块链应用的技术性能和可扩展性。

场景六：区块链技术应用于物流管理

2016 年 11 月初，欧洲最大港口鹿特丹港、荷兰银行、代尔夫特理工大学和荷兰国家应用科学研究院等组成区块链物流研究联盟，宣布共同探索区块链在物流领域的作用。

未来两年，联盟成员会联合测试物流和共同信息共享应用。代尔夫特理工大学指出，该项目会联合荷兰经济事务部的独立区块链项目，可以为联盟的测试项目提供开元基础设施。联盟成员不会单独探索区块链技术在物流行业的作用，项目核心是探索实际应用。

附件 1 专业术语

1. 比特币：比特币是一种加密数字货币，在 2009 年由化名的开发者中本聪（Satoshi Nakamoto）以开源软件形式推出。

2. 以太坊：以太坊是一个有智能合约功能的公共区块链平台。

3. 价值传输协议：用于基于互联网的价值传输。

4. Internet of Things：物联网。物联网是互联网、传统电信网等信息载体，让所有能行使独立功能的普通物体，如物理设备、汽车、建筑等实现互联互通的网络。

5. Oracle：根据预先设定的判断条件，对输入数据进行筛选，选择最适合的数据作为数据输入。

6. Data feeds：数据馈送，为区块链提供数据链下数据来源。

7. PoS：权益证明共识机制。根据每个节点所占代币的比例和时间，等比例的降低挖矿难度，从而加快找随机数的速度。

8. UTXO：未花费交易输出。比特币网络中使用的交易模型。

9. 智能合约：智能合约是由时间驱动的、具有状态的、运行在一个复制的、分享的张本质上的、且能够保管账本上资产的程序。

10. 代币：除了比特币以外的数字货币。

11. PoW：工作量证明共识机制。一方（通常称为证明人）提交已知难以计算但易于验证的计算结果，而其他任何人都能够通过验证这个答案就确信证明者为了求得结果已经完成了大量的计算工作。

12. 公有链：公有链是任何人在任何地方都能发送交易且交易能获得有效确认的、任何人都能参与其中共识过程的区块链。

13. 以太坊虚拟机：以太坊虚拟机设计运行在点对点网络中所有参与者节点上的一个虚拟机，它可以读写一个区块链中可执行的代码和数据，校

验数据签名，并且能够以半图灵完备的方式来运行代码。它仅在接收到经数据签名校验的消息时才执行代码，并且区块链上存储的信息会区分所做的适当行为。

14. 激励权益证明共识：在权益证明共识中加入了激励措施，和估计节点在线。

15. 硬分叉：区块链发生永久性分歧，在新公式规则发布后，部分没有升级的节点无法验证已经升级的节点生产的区块，通常硬分叉就会产生。

16. DAO：分布式自治组织。通过一系列公正公开的规则，可以在无人干预的和管理的情况下自主运行的组织结构。

17. 图灵完备语言：一个能计算出每个图灵可计算函数（Turing-computable function）的计算系统被称为图灵完备的。一个语言是图灵完备的，意味着该语言的计算能力与一个通用图灵机（Universal Turing Machine）相当，这也是现代计算机语言所能拥有的最高能力。

附件 2 参考文献

[1] https://en.bitcoin.it/wiki/Category:History

[2] https://panteracapital.com/wp-content/uploads/The-Final-Piece-of-the-Protocol-Puzzle. pdf
[3] https://github.com/bitcoinbook/bitcoinbook

[4] https://github.com/ethereum/wiki/wiki/White-Paper
[5] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009, https://www.bitcoin.org/bitcoin.pdf

[6] 《区块链社会解码区块链全球应用与投资案例》龚鸣 2016

[7] David Johnston et al., The General Theory of Decentralized Applications, Dapps, 2015, https://github.com/DavidJohnstonCEO/DecentralizedApplications
[8] Vitalik Buterin, Ethereum: A Next-Generation Smart Contract and Decentralized
Application Platform, 2013, http://ethereum.org/ethereum.html

[9] Paul Sztorc, Peer-to-Peer Oracle System and Prediction Marketplace, 2015, http://bitcoinhivemind.com/papers/truthcoin-whitepaper.pdf

[10] PriceFeed Smart Contract, 2016, http://feed.ether.camp/
[11] Nxt, 2013, http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt
[12] http://chainb.com/?P=Cont&id=2863
[13] http://chainb.com/?P=Cont&id=2856
[14] http://www.bochk.com/dam/bochk/desktop/top/aboutus/pressrelease2/2016/20161128_01_Press_Release_SC.pdf

[15] http://tech.sina.com.cn/i/2016-08-09/doc-ifxutfpf1573966.shtml