PointSet

新一代高性能公链，多层激励分布式信任网络

点集–技术白皮书

PointSet 白皮书（简版）

点集网络：第一个多层挖矿机制的分布式网络

说明:

此文档是 PointSet 技术白皮书 V1.2.2 版本，由点集开发团队撰写，主要介绍点集的背景、技术特点和应用场景等内容。白皮书内容可能会随项目进度更新，请访问官方网站 PointSet.org 查看最新介绍。

区块链技术在不断进步，PointSet 开发团队未来会在基金会的监督下，根据需要改进技术方案，并持续更新技术白皮书，但基础代币的发行量和分发规则保持不变。

联系我们:

Pointset （Singapore） PTE.LTD

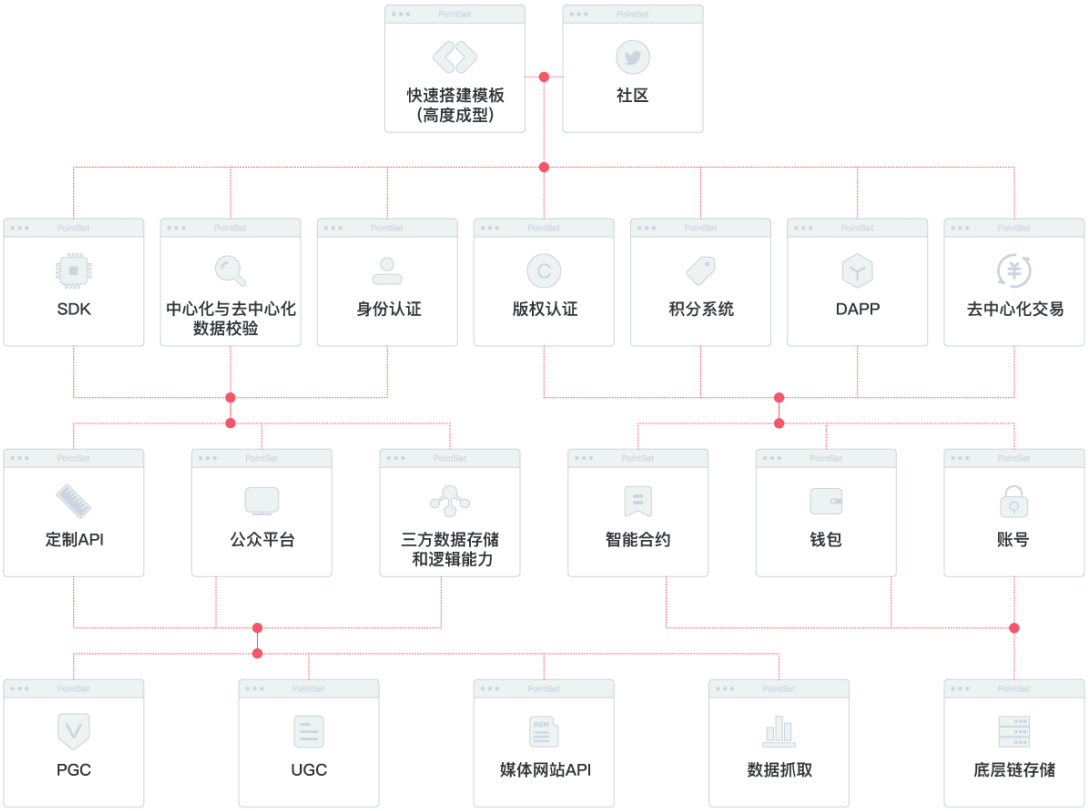
邮箱:SET@PointSet. org

一．背景：

比特币白皮书发布以来，在世界范围内被越来越多的人所接受。比特币被定义为一种完全通过点对点技术实现的电子现金系统，在比特币还没有被全世界广泛接受的时候，比特币系统中使用的区块链技术，作为一种去中心化的数据库，却能更好的应用在现实中，大大降低信任成本。相比传统互联网行业的中心化运作方式，区块链技术从比特币体系中分离出来以后，迅速的与全世界各行各业进行融合，去中心化的多人记账系统、分布式应用，使得更加安全可信。相比互联网的信息转移，区块链所实现的的价值转移，在提高运营效率、减少信任成本、参与公平性等方面有着天然的优势。

数字货币是目前世界上最方便、最公平的一种投资方式。相比传统投资，数字货币即时交易、跨国交易、手续费低等优点，大大增强了它的流动性。行情变化快、波动剧烈加上开户快捷、资金进出方便、7x24 小时交易 ，同时也是天然的投机品种。2017 年是数字货币爆发的一年，期间行情多次起起伏伏产生较大波动，比特币于年底价格达到两万美元历史高点。这一年是人们开始接受数字货币和数字资产概念的一年，经历了年初的黑客病毒事件、比特币硬分叉、ICO 热潮，以及年末的数字货币狂欢。数字货币热度空前高涨，还有指标显示出数字货币强大的自我营销力：算力快速上涨、TOKEN 数量爆发式增长、比特币占比下降。我们相信未来世界里一定有数字货币的一席之地。

二．PointSet 技术介绍



点集(PointSet)作为一个底层网络，以分布式技术为基础，构建一个去中心化网络体系。从底层数据多渠道获取和高性能存储，到中间层数据的处理和链上记录，再到应用层提供 api 和 sdk，为开发者和用户构建底层数据与上层应用的桥梁，在信息交换和价值转移上发挥着重要的作用。通证经济模型下的 SET 作为整个生态的价值转移媒介，多层挖矿机制能够保证整个生态的良性循环。

1.SETChain

PointSet 链应用最新一代技术开发，为普通用户、开发者、网站、第三方伙伴、平台、组织等多元渠道提供面面俱到的链上数据记录

（身份认证、版权保护、激励机制等）。

PointSet 链上每个数据都是一个 Point，无数个 Point 构成了一个 Set。链上包含智能合约，开发者能快速搭建自己的 DAPP；也可以通过点集网络上层的 PointDock 快速集成。

除了现有的主链技术外，PointSet 还自创改进了包括 PointCheck、PointDock、PointPaxos 在内的一系列基础设施，为生态数据的安全保驾护航

2.区块

SET 块的构成大量借鉴了优秀主链的构造，包含以下部分内容：

a) ParentHash 父区块的哈希

b) stateRoot： 当前已定稿区块的交易组成的状态数根节点的哈希

c) transactionRoot: 交易树根节点的哈希

d) receiptRoot：收据树根节点的哈希

e) logsBoom：所有交易收据中的可索引信息组成的布隆过滤器

f) difficulty：打包当前区块的难度纯量值

g) number：区块的祖先的数量

h) timestamp：区块初始化的时间戳

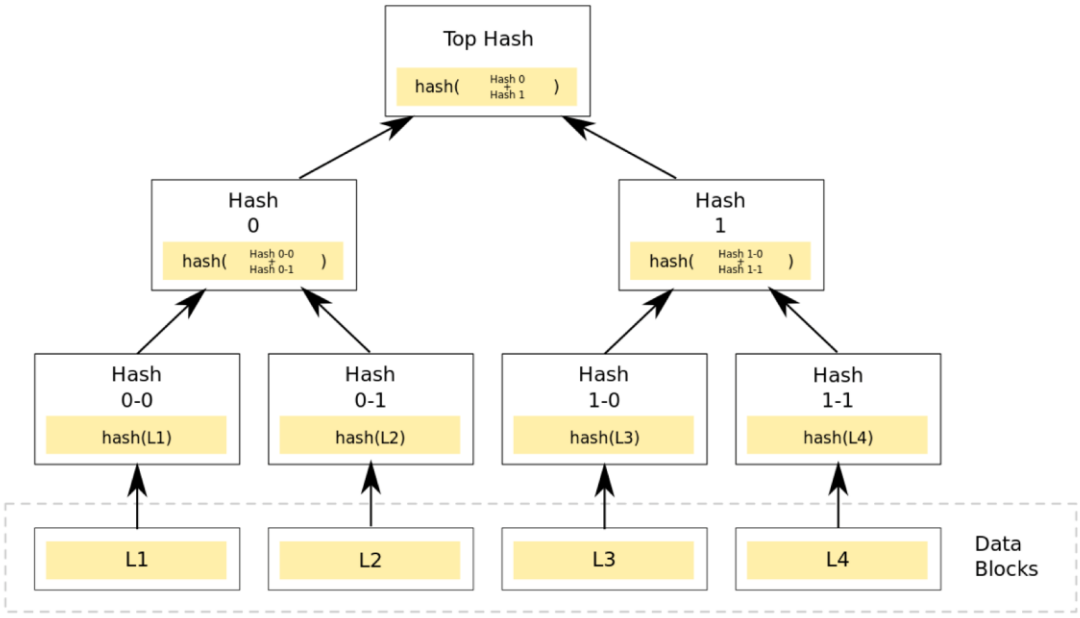
i) extraData：对当前区块的备注

j) mixHash：256 位哈希

k) nonce：64 位值（和 mixHash 共同证明计算量的承载是否足

够)

其中交易树和收据树都是 Merkle 树，默克尔树：



Merkle Tree 可以看做 Hash List 的泛化（Hash List 可以看作一种特殊的 Merkle Tree，即树高为 2 的多叉 Merkle Tree)。

在最底层，和哈希列表一样，我们把数据分成小的数据块，有相应地哈希和它对应。但是往上走，并不是直接去运算根哈希，而是把相邻的两个哈希合并成一个字符串，然后运算这个字符串的哈希，这样每两个哈希就结婚生子，得到了一个”子哈希“。如果最底层的哈希总数是单数，那到最后必然出现一个单身哈希，这种情况就直接对它进行哈希运算，所以也能得到它的子哈希。于是往上推，依然是一样的方式，可以得到数目更少的新一级哈希，最终必然形成一棵倒挂的树，到了树根的这个位置，这一代就剩下一个根哈希

了，我们把它叫做 Merkle Root。

在 p2p 网络下载网络之前，先从可信的源获得文件的 Merkle Tree 树根。一旦获得了树根，就可以从其他从不可信的源获取 Merkle tree。通过可信的树根来检查接受到的 Merkle Tree。如果 Merkle Tree 是损坏的或者虚假的，就从其他源获得另一个 Merkle Tree，直到获得一个与可信树根匹配的 Merkle Tree。

Merkle Tree 和 Hash List 的主要区别是，可以直接下载并立即验证 Merkle Tree 的一个分支。因为可以将文件切分成小的数据块，这样如果有一块数据损坏，仅仅重新下载这个数据块就行了。如果文件非常大，那么 Merkle tree 和 Hash list 都很到，但是 Merkle tree 可以一次下载一个分支，然后立即验证这个分支，如果分支验证通过，就可以下载数据了。而 Hash list 只有下载整个 hash list 才能验证。

默克尔树能快速的定位树叶的改变，大量节省查询耗时。
而交易状态树是默克尔帕特里夏树（MPT）:
MPT（Merkle Patricia Tree）顾名思义，MPT 就是默克尔树和葩特里夏树的混合体:
在 SET 链中，我们使用一种十六进制的前缀编码，字母表中存在 16 个字符，其中已一个字符为 nibble

MPT 树中的节点包括空节点、叶子节点、扩展节点和分支节点:

空节点，简单的表示空，在代码中是一个空串。

叶子节点（leaf），表示为[key,value]的一个键值对，其中 key 是 key 的一种特殊十六进制编码，value 是 value 的 RLP 编码。

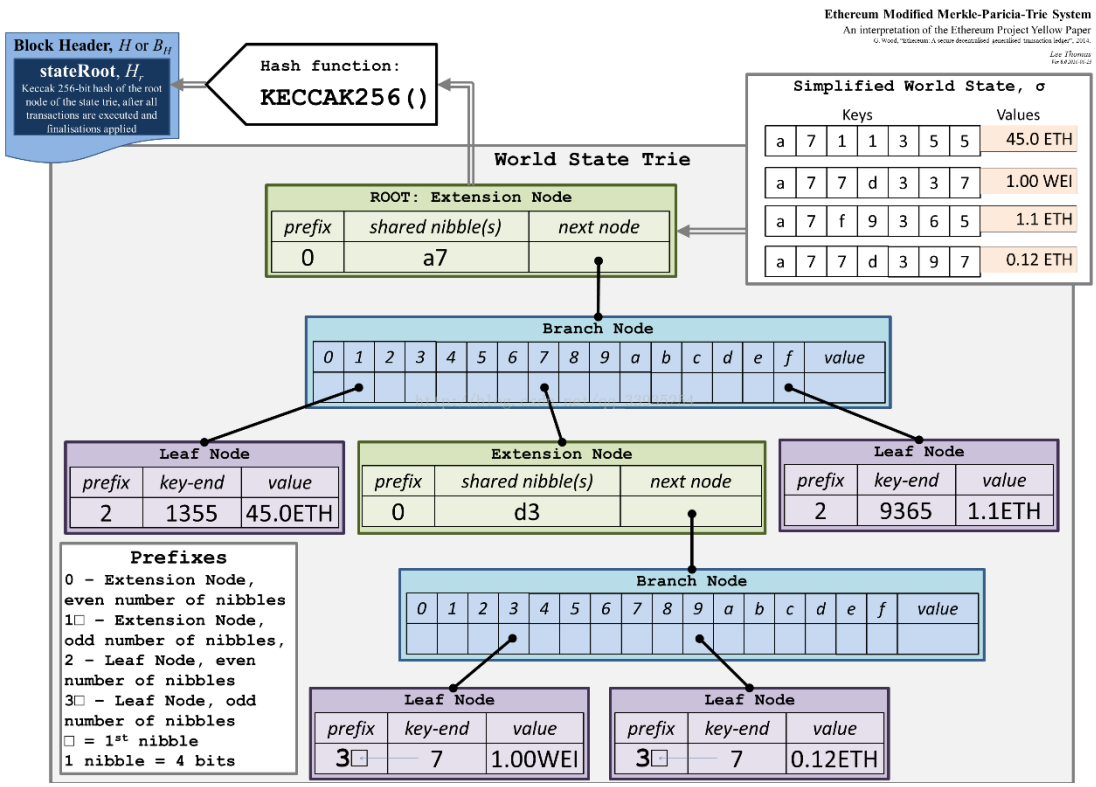
扩展节点（extension），也是[key，value]的一个键值对，但是这里的 value 是其他节点的 hash 值，这个 hash 可以被用来查询数据库中的节点。也就是说通过 hash 链接到其他节点。

分支节点（branch），因为 MPT 树中的 key 被编码成一种特殊的 16 进制的表示，再加上最后的 value，所以分支节点是一个长度为 17 的 list，前 16 个元素对应着 key 中的 16 个可能的十六进制字符，如果有一个[key,value]对在这个分支节点终止，最后一个元素代表一个值，即分支节点既可以搜索路径的终止也可以是路径的中间节点。

MPT 树中另外一个重要的概念是一个特殊的十六进制前缀(hex-prefix, HP)编码，用来对 key 进行编码。因为字母表是 16 进制的，所以每个节点可能有 16 个孩子。因为有两种[key,value]节点(叶节点和扩展节点)，引进一种特殊的终止符标识来标识 key 所对应的是值是真实的值，还是其他节点的 hash。如果终止符标记被打开，那么 key 对应的是叶节点，对应的值是真实的 value。如果终止符标记被关闭，那么值就是用于在数据块中查询对应的节点的 hash。无

论 key 奇数长度还是偶数长度，HP 都可以对其进行编码。最后我们注意到一个单独的 hex 字符或者 4bit 二进制数字，即一个 nibble。

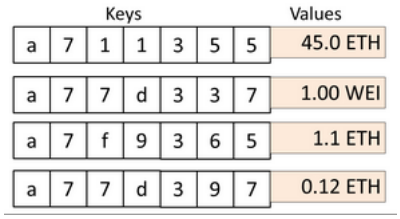
HP 编码很简单：一个 nibble 被加到 key 前（下图中的 prefix），对终止符的状态和奇偶性进行编码。最低位表示奇偶性，第二低位编码终止符状态。如果 key 是偶数长度，那么加上另外一个 nibble，值为 0 来保持整体的偶特性。



如图所示:

总共有 2 个扩展节点，2 个分支节点，4 个叶子节点。

其中叶子结点的键值情况为：



节点的前缀：

```
    PreFixes
0 - Extension Node,
even number of nibbles
1 - Exstension Node,
odd number of nibbles,
2 - Leaf Node,
even number of nibbles
3 - Leaf Node,
odd number of nibbles
 = 1^st nibble
1nibble = 4 bits
```

交易树、状态树、收据树记录了区块上最重要的信息，也是防止区块不被篡改和方便验证的核心所在。

在本区块记录父区块的哈希是连接整个链完整的必要条件。

3.SET 激励

无论是 pos 或者 dpos 的共识机制，我们都需要激励机制维护整个主链的正常运行，我们设计了一种一致同意的转一家之方法，PointSet 主链尾了解决这个问题，设计了一种内置的货币—SET，运行在 set 主链上的所有货币都以 point 为最小单位计算

a) Token 的最小单位是 point，1SET = 10^18point

b) 第二个单位是 line，1SET = 10^15 line

c) 然后是 flat，1SET = 10^12 flat

d) 最大的单位为 SET

4.PointCheck

a) PointSet 具有版权校验、内容记录等功能，数据源来自 PGC、UGC 、媒体等多种渠道。在 SimHash 和 SimHash 的基础上调整为 PointCheck，通过判断用户提交的版权内容的相似性,计算其权重得出结论（是否储存合法以及判断对应的奖励)。

b) SimHash 通过以下流程计算出两个文档之间的相似性：

1）分词

将文档分词，然后为每个词分配权重（比如可以用 tf-idf 算法计算权重，但这里需要变换一下算法，将 tf-idf 值以单调递增函数映射到一个整数值)

2）计算 Hash

3）加权

将词乘以对应的权值，0 用-1 代替乘以对应权值

4）合并

把单词序列从前到后按位累加

5）降维

把合并的结果变为 0-1 串，方法是大于 0 的—>1，小于 0 的->0，

这样每篇文档会得到一个 ID

6）比较海明距离

将降维后得到的结果与已有的每一篇文档的 ID 做异或运算，然后求运算结果中 1 的个数，得到海明距离。

SimHash 算法高效，适用于分布式当中，消耗空间小，但是长短文档同时存在时，会有误判的情况。

MinHash 在前期的处理上和 SimHash 很相似，但是在 binary data 的判断效率上明显超过 SimHash：

$$Pr(h_{\pi}^{min}(W_1) = h_{\pi}^{min}(W_2)) = \frac{|W_1 \cap W_2|}{|W_1 \cup W_2|} = \mathcal{R}.$$

PointCheck 从两种 hash 相似判断的基础上优中取优，在进行 binary 判断上使用 MinHash，其它的使用 SimHash，在提高效率的同时，高度提高了判别的准确性。

5.PointDock

Point Dock 是一整套接入系统。点集网络不仅可以对接项目方、媒体平台，还会接入自媒体甚至普通用户。

Point Dock 有如下体系：

a）积分系统，即便是普通用户都可以接入 PointSet，在经过身份

绑定之后，用户或者平台随时可以将文档储存到 PointSet 上，经过 PointCheck 校验之后，得出对应的结果，返还你对应的积分。

b）自媒体接入，PointSet 将打通微信公众号、头条号等媒体。在进行过身份绑定之后，可以进行版权校验保护、积分赠送等其它操作。

c）低成本 WEB 搭建，为了方便第三方接入者更专注于运营等方面的业务，我们汇集成一整套网站模板，其中将包含 PointSet 完备的激励系统、身份认证系统、版权保护系统，而使用 PointSet 身份认证系统的普通用户也将减少注册成本、数据打通，实现从 Point 到 Set 的完美集合。

d）普通开发者，普通开发者可以接入可定制度更高的 API，开发者可以仅仅使用身份系统，零成本获取 PointSet 用户，更可以选择性的接入点集网络的积分系统、版权系统等其他模块。

e）深入合作开发者，PointSet 将开放更多权限给深入合作开发者，共同探讨区块链世界，创造更大的社会价值。

6.SET 共识机制

由于 pow 共识机制一直存在浪费资源、效率低下、TPS 不高的问题，所以我们采用更加快速、安全且能源消耗比较小的 dpos 算法。

DPOS 即委托股权证明——它是权益证明(以太坊的 PoS)的一种变体，以限制网络上验证者的数量为代价，提供高级别的可扩展性。

根据这种算法，pointset 全网持有代币的人可以通过投票系统来选择区块生产者，一旦当选任何人都可以参与区块的生产。有点像“人民代表大会制度”，由所有加入 pointset 网络的节点中选取 10 个超级节点，再由这些超级节点之间进行 pointset 区块链的共识，也正因超级节点的存在大大提高了 pointset 链的 TPS。

在 POW 或者其他的 POS 共识里，节点不限、随机出块顺序的问题，任何加入 pointset 网络的节点都有成为超级节点的存在，而超级节点需要其他所有普通节点进行投票选举的，当然超级节点也具有一定的职责：

1.提供一台服务器节点，保证节点的正常运行；

2.节点服务器收集网络里的交易；

3.节点验证交易，把交易打包到区块；

4.节点广播区块，其他节点验证后把区块添加到自己的数据库；

5.带领并促进区块链项目的发展；

如果超级节点不能按时履行自己的职责，就会立马被换掉，由其他正在竞争的投票数高的节点竞选上去，以此高效维护 pointset 区块链平台的正常运转。

DPOS 解决的拜占庭容错从两个维度降低了难度：

1、节点数量固定只有 21 个。并且节点信息透明。

2、固定出块顺序。每个节点跟接力棒一样，一个个往下接力出块。

每个节点不能还没轮到它出块的时候，就出块。都是必须轮到再出块。如果出现出块故障，会跳过这个节点。

DPOS 共识过程：

只要能获得 token 持有者的投票，任何人都可以参与区块的生产过程，也有机会独立的生产区块。pointset 区块链上预计每 1.5 秒生产一个区块。任何时刻，只有一个生产者被授权产生区块。如果在某个时间内没有成功出块，则跳过该块。

使用 Pointset 客户端软件全节点模式，区块以 100 个区块为一轮（每个生产者可以生产 10 个，有 10 个生产者，二者相乘)。在每十轮的开始，10 个区块生产者通过 token 持有者的投票被选中。选中的生产者依据商定好的顺序生产区块，这个顺序由 10 个或者更多的生产者商定。

pointset 架构中区块产生是以 10 个区块为一个周期。在每十个出块周期开始之前，10 个区块生产者会被投票选出。前 9 名出块者首选自动选出，第 10 个出块者按所得投票数目对应概率选出。所选择的生产者会根据从块时间导出的伪随机数进行混合。以便保证出块者之间的连接尽量平衡。

如果出块者错过了一个块，并且在最近 3 小时内没有产生任何块，

则这个出块者将被删除。通过不安排那些不够可靠的节点，尽可能的减少错过区块创建，来让整个网络运行得更平稳。

在正常情况下，DPOS 块链不会经历任何叉，因为块生产者合作生产区块而不是竞争。如果有区块分叉，共识将自动切换到最长的链条。具有更多生产者的区块链长度将比具有较少生产者的区块链增长速度更快。此外，没有块生产者应该同时在两个区块链分叉上生产块。如果一个块生产者发现这么做了，就可能被投票出局。

交易确认

由 DPOS 共识算法维护的区块链一般出块者都是 100%在线的。这就是说一个交易平均 0.5 秒后，会被写入区块链中，同时被所有出块节点知晓这笔交易。这就意味着只需要 0.5 秒，一笔交易可以认定为 99.9%被区块链接收了。

在常规的情况下，DPOS 区块链不太可能会产生分叉，因为区块的生产过程是一个合作的过程而不是一个相互竞争的过程。如果产生的分叉，共识将会自动转向最长的链。这一机制有效是因为一个区块被加入到区块链的速率与区块生产者的数量直接相关，而这些生产者都对这个最长链条达成共识。换句话说，一个分叉的区块链，如果有更多的生产者，长度将会比更少的生产者更快，因为更多生产者的那条链上错过创建的区块数要少很多。

有一些非常情况下例如，软件 bug，Internet 拥塞或恶意出块者出现，区块链可能出现分叉。为了确保一个交易是不可逆转的，可以等待 10 个区块确认。根据 pointset 链的配置，在正常情况下 10 个区块确认平均需要 15 秒。

在分叉产生的 9 秒钟内，出块节点就可能发现这个分叉可能并警告用户。一个节点观察网络的时候如果发现连续 2 次的丢块事件，这意味着改节点由 95%可能性在区块链的分叉分支上。有出现 3 个连续的丢块以后，该节点有 99%的可能性在一条分叉出来的区块链上。可以生成一个预测模型，它将利用节点丢失的信息，最近的参与率以及其他因素来快速地警告用户出现什么问题。
对这种警告的反应完全取决于业务交易的性质，但最简单的反应是等待 7/10 确认，直到警告停止。

交易证明（TaPoS）
pointset 要求每个交易都包括最近的区块头的哈希。 这个哈希有两个目的：

1.防止分叉区块链上出现大量交易记录;

2.使得系统能感知到用户是否在分叉出来的区块链上

随着时间的推移，所有用户最终直接确认块链，这使得难以伪造假冒链，因为假冒将无法从合法链路迁移交易。
DPOS 共识的最基本原则：

a) 用户会根据自己手里的具有可投票权的币持有量做出带有权重的投票，根据投票结果，按照一定的规则选择出当前的超级节点生成区块；

b) 同时，竞选超级节点而落选的节点、投票给中选者的用户、投票给落选者的用户均可能获得一定量的补偿，以激励他们持续参与之后的竞选流程；

c) 超级节点会按照一定的分配规则依次进行区块的打包并获得最大份额的奖励；

d) 超级节点中的多数会根据投票结果进行选择，剩下的会按照一定的算法保证在余下的其他节点中，所有节点都有可能被选中。

7.智能合约

智能合约全部由代码组成，而典型的合同则是一份有着法律意义的文本，它最大的特点就是无法更改和自动执行，这构成了智能合约实现“匿名信用”的基础。

智能合约主要有四个目的：存储和维护数据、管理不可信用户之间的合约/关系、作为软件库为其他合约提供函、支持复杂权限管理。大家看其实很通用，并没有针对某些特定的应用做优化，并且以上特性可以组合使用。这是 pointset 一直坚持的，做一个最基本、对代码执行机制的支持。

区块链智能合约有三个技术特性：

1. 数据透明

区块链上所有的数据都是公开透明的，因此智能合约的数据处理也是公开透明的，运行时任何一方都可以查看其代码和数据。

2. 不可篡改

区块链本身的所有数据不可篡改，因此部署在区块链上的智能合约代码以及运行产生的数据输出也是不可篡改的，运行智能合约的节点不必担心其他节点恶意修改代码与数据。

3. 永久运行

支撑区块链网络的节点往往达到数百甚至上千，部分节点的失效并不会导致智能合约的停止，其可靠性理论上接近于永久运行，这样就保证了智能合约能像纸质合同一样每时每刻都有效。

智能合约的工作原理

智能合约模块，pointset 将会实现自己的以 Web Assembly 为基础的虚拟机 pvm，用户可以用各种主流语言 c、c++、python、java 等来开发自己的智能合约，从而定制化的满足用户需求。智能合约最终运行在虚拟机上，开发者们便可以实现复杂多样的功能，满足定制化需求。

开发人员会为智能合约撰写代码。智能合约可用于交易和（或）两方 / 多方之间的任何交换行为。该代码包含一些会触发合约自动执行的条件。

一旦编码完成，智能合约就会被上传到区块链网络上，即它们被发送到所有连接到网络的设备上。从另一种区块链应用——比特币——的情况来说，这就好像把关于比特币交易的网络更新上传到区块链上。

一旦将数据上传到所有设备上，用户就可以与执行程序代码的结果达成协议。然后更新数据库以记录合约的执行情况，并监督合约的条款以检查合规性。

这样一来，单独一方就无法操纵合约，因为对智能合约执行的控制权不在任何单独一方的手中。

与传统合约相比，智能合约有很多优势：

i. 智能合约与传统合约相比，最大的特点和优势就是其解决了“信用”的问题。传统合约达成前，参与者先要了解各方的信用背景以选择合适的对象，合约达成后的阶段，也要依赖于各方的诚实信用，或者引入第三方（如支付宝）来担保合约履行。

ii. 智能合约因为链上的资源是真实透明的，合约的内容确定后就无法更改，执行更是不用依赖任何额外操作。最终，“匿名信用”成为现实，合约缔结前无需进行信用调查，缔结后也不用第三方进行担保履行，从而实现交易成本大大降低，交易效率

则大幅提高

iii. 智能合约的数据无法删除、修改，只能新增，而智能合约的历史可追溯，同时篡改合约或违约的成本将很高，因为其作恶行为将被永远记录并广为人知。

iv. 去中心化的智能合约，不依赖第三方执行合约。因此，智能合约的潜在好处包括降低签订合约、执行和监管方面的成本；因此，对很多低价值交易相关的合约来说，这是极大降低人力成本。合约验证和执行的整个过程随着用户间的直接交易而变得快速。

v. 智能合约不容易出现断电、节点故障、水灾火灾等问题。智能合约保存在区块链分布式账本上时，不存在放错或丢失的风险。这意味着连接到网络的每个设备都有一份合约副本，并且数据会永远保存在网络上。

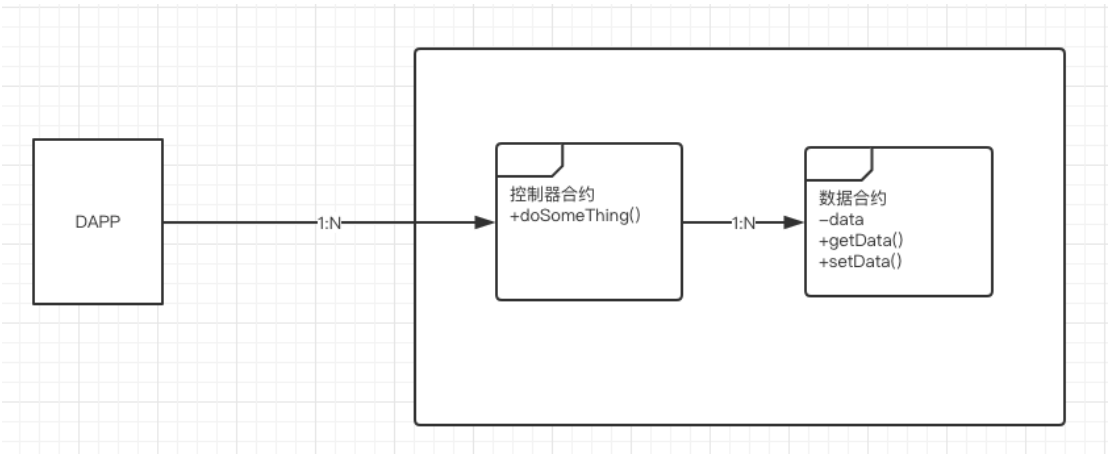
8.CD（Controller-Data）模式

从业务视角来看，智能合约只需要做两件事，其一是如何定义数据的结构和读写方式，其二是如何处理数据并对外提供服务接口。

为了更好的做好模块抽象和合约结构分层，将这两件事分开，既是将业务控制逻辑和数据从合约代码层面就做好分离，这样的处理在

复杂业务逻辑场景中经过实践是当前被认为最佳的模式。

这个模式简称为 CD（Controller-Data）模式。将合约分为两类：控制器合约（Controller Contract）与数据合约（Data Contract）。



控制器合约通过访问数据合约获得数据，并对数据做逻辑处理，然后写回数据合约，它专注于对数据的逻辑处理和对外提供服务。

根据处理逻辑的不同，常见的有命名空间控制器合约、代理控制器合约、业务控制器合约、工厂控制器合约等。一般情况下，控制器合约不需要存储任何数据，它完全依赖外部的输入来决定对数据合约的访问。特殊情况下，控制器合约可以存储某个固定的数据合约的地址或者命名空间（通过命名空间在运行时获得合约地址）。

数据合约专注于数据结构定义与所存储数据的读写裸接口。为了达到数据统一访问管理和数据访问权限控制的目的，最好是将数据读

写接口只暴露给对应的控制器合约。禁止其他方式的读写访问。

基于这个模式，遵循从上至下的分析方式，从对外提供的服务接口开始设计各类控制器合约，再逐步过渡到服务接口所需要的数据模型和存储方式，进而设计各类数据合约，可以较为快速的完成合约架构的设计。

9.SETRLP

RLP（递归长度前缀)提供了一种适用于任意二进制数据数组的编码，RLP 是 SET 主链中对对象进行序列化的主要编码方式。 RLP 的唯一目标就是解决结构体的编码问题；对原子数据类型（比如，字符串，整数型，浮点型）的编码则交给更高层的协议；我们规定 SET 中数字必须是一个大端字节序的、没有零占位的存储的格式（也就是说，一个整数 0 和一个空数组是等同的)。对于在 RLP 格式中对一个字典数据的编码问题，有两种建议的方式，一种是通过二维数组表达键值对，比如[[k1,v1],[k2,v2]...]，并且对键进行字典序排序。

10.SET 网络协议

区块链技术的去中心依赖于底层组网技术，PointSet 的底层实现了 p2pServer，大约可以分为这样三层。

a) 底层路由表。封装了 kad 路由，节点的数据结构以及计算记录，节点搜索，验证等功能。

b) 中层 peer 抽象，message 开放发送接口，server 对外提供

peer 检测，初始化，事件订阅，peer 状态查询，启动，停止等功能

c) PointSet 最上层 peer，peerset 再封装，通过协议的 Run 函数，在中层启动 peer 时，获取 peer，最终通过一个循环截取稳定 peer，包装在 peerset 中使用。

底层路由表

这里简化问题仅讨论 Node Discovery Protocol。 这一层维护了一个 buckets 桶，总共有 17 个桶，每个桶有 16 个节点和 10 个替换节点。 Node 放入时先要计算 hash 和 localNode 的距离。再按距离选择一个桶放进去，取的时候逐个计算 target 和每个桶中对象的举例，详细参考 closest 函数，后面会贴出来。

距离公式满足：f(x,y)=256-8*n-map(x[n+1]^y[n+1]) 注：n 为相同节点数量 map 为一个负相关的映射关系。

简单来说就是相似越多，值越小。

其中最重要的就是 table 对象，table 公共方法有：

a) newTable 实例创建

b) Self local 节点获取

c) ReadRandomNodes 随机读取几个节点

d) Close 关闭

e) Resolve 在周边查找某个节点

f) Lookup 查找某个节点的邻近节点

11.SETRPC

RPC 规定在网络传输中参数和返回值均被序列化为二进制数据，这个过程被称为序列化（Serialize）或编组（marshal）。通过寻址和传输将序列化的二进制发送给另一台服务器。另一台服务器收到二进制数据以后会反序列化，恢复为内存中的表达方式，然后找到对应方法调用将返回值仍旧以二进制形式返回给第一台服务器，然后再反序列化读取返回值。

三. 点集网络(PointSet) 应用场景

1. 数字身份

互联网时代的个人信息在隐私性、安全性和易用性等方面不够合理。在点集网络中个人可以创建自己的身份，完全掌控并保证该身份的真实性和安全性。个人数字身份就是一个打开区块链世界的钥匙，有了这把钥匙，用户可以用来进行签署协议、保护版权、参与投票、交易资产等活动。

2. 版权保护

互联网的出现大大加速了信息传播速度，但是也带来了一些副作用。当前互联网经济模式下，版权保护一直是互联网时代的重点，版权保护的缺失造成了版权保护难、版权举证难、版权维权难。

利用点集链以及点集身份系统，点集网络提供了一套安全、便捷、低成本的版权保护系统。在点集网络中，内容生产者可以通过身份系统建立自己的唯一数字签名，作品绑定数字签名后，这些不可篡改的记录在去中心化底层网络中存储，使得内容生产者的版权得到区块链认可，方便于版权举证、维权。

3. 分布式社交网络

在点集的去中心化社交网络里，用户可以自己控制自己的数据，利用数字身份系统，用户可以自行运行节点接入网络，节点之间实时链接，用户信息端对端加密存储在公链上，社交信息在公链上是冗余存储，该信息只有私钥持人自身能查看。点集分布式社交网络把用户信息控制权归还给用户，保障用户隐私。

代币的激励机制可以激励用户创造更多的价值，点集网络作为一个数据平台，可以实现用户跟用户之间点对点交流，没有第三方介入。用户可以选择好友之间的正常通讯交流，也可以选择匿名聊天，还可以在平台上创建社群，完全取决于掌控私钥的用户自己。

4、分布式内容平台

传统媒体经济模型由用户、作者、平台、广告商多方组成，每一方需求都是不统一的。用户可以使用平台功能满足信息、关系等需求，

但是用户对于平台没有控制权和收益权，在整个经济体系中，用户始终处于一个被动状态。

点集网络弱化了各方参与者的角色概念，在符合参与者利益最大化的前提下，角色身份可以互相转化。除了为开发者提供 api 等接口外，用 token 激励机制提出一个全新的概念——用户即所有。用户既是生产者也是消费者，同时又是广告方。参与底层开发建设的用户也可以是平台方，符合区块链人人参与的去中心化精神。

利用点集可以构建一个去中心化内容生产和激励生态的网络，使得内容生产者、内容消费者、内容平台方以及广告方各方面资源合理分配，获得合理的回报。点集网络在版权保护、用户需求、广告投放等方向都有着非常广阔的前景。

5、其他应用场景

去中心化资产服务

去中心化交易

去中心化保险

资产链上流动

商品溯源

公益慈善

……

PointSet 一个多层挖矿机制下的公链，以点集链为出发点，主打应用是数字身份、版权保护、去中心化社交以及分布式内容平台，
之后会拓展到去中心化资产服务、去中心化交易等方面。未来点集网络将融合跨链存储功能，将给整个系统带来质的飞跃。

四. 通证激励

1. PointSet 代币 SET

点集网络的生态建立离不开代币激励机制。SET 是点集网络中的代币，总 量：21000000000 永不增发。
合约地址：0xd2C6738D45b090ec05210fE8DCeEF4D8fc392892

３０％的 SET 用来构建生态挖矿池。生态是点集网络的根本，点集网络采用独创动态算法 SET Method(结合 Delphi Method+ahp method)开发者生态贡献值，按照权重分配挖矿收益，以此运行点集网络的双层挖矿机制和代币销毁机制。
２０％的 SET 用来团队激励。
20%基金会份额用于商业合作、生态发展等途径。
30%用于代币兑换以及糖果发放。

SET 所兑换 ETH 全部用于项目建设。包括开发团队人才引进、市场拓展、社区运营等方面。

2. 销毁机制

SET 设计初衷是一个小幅度通缩的激励代币，在永不增发的前提下，将对 PointSet 生态内 dapp 的所获收益，收取一定比例的佣金，这部分佣金也按照比例进行回购 set 销毁。

六 、团队和合作伙伴

1. 核心建设者

PointSet 团队成员均来自百度、阿里巴巴、网易、马蜂窝等知名互联网公司，大多数是国内早期区块链项目布道者、投资者。 团队深谙互联网创业和区块链投资，在区块链领域具有前瞻的全球化眼光和全球化业务管理经验，擅长商务拓展与市场战略性规划。其中技术负责人热衷于区块链技术，对区块链数据存储、数字身份、版权保护、数字资产安全等方面颇有研究。团队成员目标一致，努力开发 PointSet 底层构架，把 PointSet 推向数字经济领域的顶峰。

Mateo

点集（新加坡）创始人&首席执行官

Gotop.vc 冲顶资本创始人

经济学学士，多年私募股权、投资银行工作经验；资深数字货币投资人，擅长团队、项目管理；丰富的区块链解决方案及区块链落地项目经验。

https://www.linkedin.com/in/mateo-pointset/

Jorge

点集（新加坡）技术总监

负责 Pointset 整体产品规划和研发工作，多年计算机软件开发从业经验，曾供职于国内大型视频通讯科技公司，对网络优化、高并发以及分布式系统的开发有着丰富的经验。专注于区块链的底层存储优化，致力于解决区块链的三元悖论。

https://www.linkedin.com/in/set-Jorge/

Pedro

点集（新加坡）设计总监

多年的知名互联网公司设计师。擅长用户体验、交互设计，有多个知名产品上线。

www.linkedin.com/in/set-pedro

Pandrea

点集（新加坡）商务经理

区块链投资早期参与者，人脉资源广泛，有丰富的融资经验，负责点集生态建设、商务市场拓展。

www.linkedin.com/in/set-Pandrea

Lucas

点集（新加坡）运营总监

擅长移动互联网产品设计，熟悉区块链底层的多个项目产品逻辑，在内容存储，版权保护方面颇有研究。多年互联网产品运营经验，掌握多种语言，拥有广泛的市场营销和管理经验。

https://www.linkedin.com/in/set-lucas/

Miguel

点集（新加坡）研发经理

全栈工程师，擅长技术构架设计、多年知名互联网企业工作经验，区块链领域颇有建树。

https://www.linkedin.com/in/set-miguel/

2. 合作伙伴

比特派(bitpie.com)是由比太团队(bither.net)研发的新一代区块链资产综合服务平台，立足于 HD 钱包技术、多重签名和链上交易，让你轻松安全的使用数字货币，轻松发送和接收比特币,还能方便的进行各类交易。

拓扑链是区块链游戏全球领军品牌，以去中心化理念重塑游戏行业体系结构，通过拓扑链玩家社区、拓扑共识、拓扑挖矿三大共识方案解决当前游戏行业巨头垄断、渠道积弊，构建多方共赢的去中心化产业结构。

Coinjapan 是通过众筹吸引日本投资的可靠合作伙伴。世界上最大的加密货币市场拥有积极的投资者，他们愿意投资创新项目和未来的技术，只对那些用可理解的语言“说话”的人开放。Coinjapan 将为贵公司的日本投资市场铺平道路，并为项目的快速发展提供成功的 ICO。

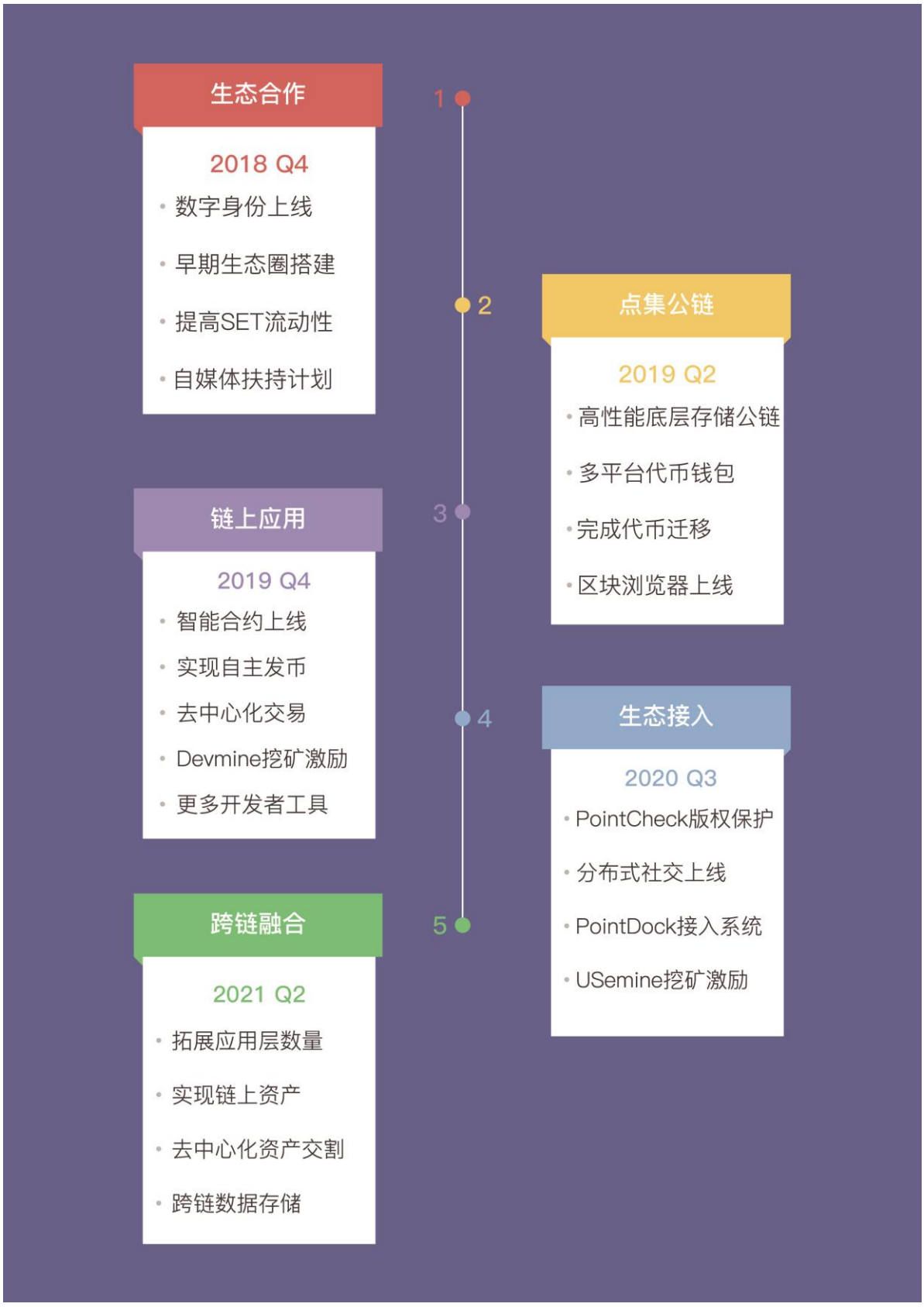
铂金区是一个网络营销公司，由它最强大的电子邮件营销解决方案有助于您的业务收入。世界正变得无国界，在未来拓展业务，你必须专注于世界发展水平，以支持不断扩大的边防总队，并建立位置与全球性公司。

冲顶资本，专业区块链投资机构。

币财经是一个集资讯、行情数据、导航、项目库、策略选币等功能为一体的区块链服务平台，及时的资讯、准确的数据和实用的工具，为区块链投资之旅保驾护航。

一键进入币圈儿世界，发红包、看资讯、聊天灌水应有尽有。

七. 项目规划


生态合作
1
2018 Q4
• 数字身份上线
• 早期生态圈搭建
• 提高SET流动性
• 自媒体扶持计划
2
点集公链
2019 Q2
• 高性能底层存储公链
• 多平台代币钱包
• 完成代币迁移
• 区块浏览器上线
链上应用
3
2019 Q4
• 智能合约上线
• 实现自主发币
• 去中心化交易
• Devmine挖矿激励
• 更多开发者工具
4
生态接入
2020 Q3
• PointCheck版权保护
• 分布式社交上线
• PointDock接入系统
• USemine挖矿激励
跨链融合
5
2021 Q2
• 拓展应用层数量
• 实现链上资产
• 去中心化资产交割
• 跨链数据存储

八. 风险提示和免责声明

1. 注意事项

本文档仅用于传达信息用途，所有信息不构成任何关于证券形式的投资建议或教唆投资。本文档不组成也不应被理解成为提供任何买卖的行为，也不是任何形式上的合约或者承诺。

本文不涉及任何在司法管制内的受管制产品，本文件是项目阐述的概念性文件【白皮书】，并非出售或者征集招标与 PointSet 产品及其相关公司的股份、证券或其他受管制产品。

所有参与者均具备一定的抗风险能力，属于合格投资人，请做好风险评估并结合自身风险承受能力参与 PointSet。PointSet 团队明确表示相关用户充分了解所存在的风险，用户一旦参与投资即表示了解并接受该项目风险并愿意个人为此承担一切相应结果或后果。

2. 风险提示

由于区块链行业还处于十分早期的发展阶段，各国政府对区块链与加密数字货币行业的监管态度尚不十分明朗，存在诸多的不确定性风险。本项目有因政策不确定性、市场需求、技术性或者其它不可控的因素导致项目开发失败的可能，项目失败的最差后果可能会导致您投入的所有比特币或者其它币无法收回。

参与 PointSet 众筹的合格投资人，请仔细阅读 PointSet 项目介绍，

认清参与合伙人计划所存在的潜在风险，并充分评估自己的风险承受能力和实际情况，进行理性判断。

PointSet 的未来基于区块链技术和密码学算法构建，目前区块链技术仍然是一项非常早期的技术，密码学也一直处于高速发展的过程中，PointSet 团队不能完全确保所有技术的顺利落地，同时所有的技术类项目都具有被黑客攻击或代码漏洞造成用户损失的可能。

除上述风险外，由于加密货币投资仍然是一个崭新的领域，可能还有各种我们尚未提及或尚未预料到的风险。