GROWCHAIN

基于区块链打造全球母婴行业新生态

白皮书 2.0

2018,01

目录

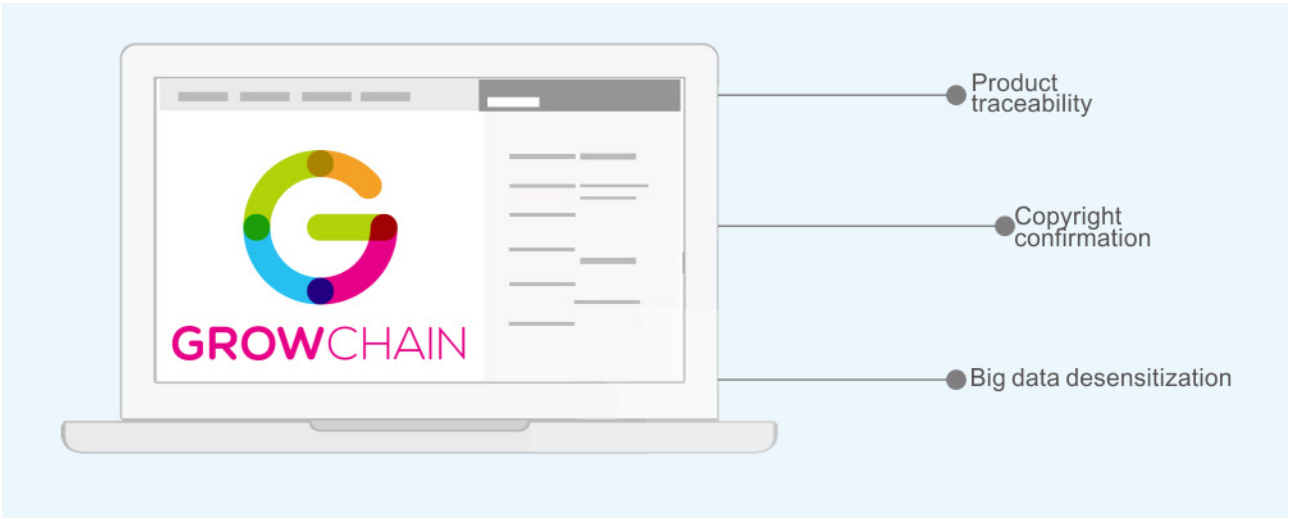
一、摘要

Growchain（成长链）是基于区块链技术打造的一个去中心、去信任的母婴应用平台，也是**全球首个母婴行业垂直公有链**。Growchain 旨在颠覆传统的母婴行业规则，构建一个安全、公平、可靠的专注于全球母婴行业的全新生态。

在这个全新的生态系统中，区块链技术将被用以重塑整个母婴行业的信任机制。区块链的分布式数据存储、匿名、不可篡改等特性将会充分的应用于母婴市场中的成长档案、创作生态、大数据脱敏等多个方面，合理改善了数据丢失、数据伪造、数据泄漏等问题。

Growchain 团队的初衷是通过对去中心化母婴商业平台的搭建和维护，与优质应用和内容的合作，为全球母婴用户提供一个安全透明、数据可靠、内容丰富，同时关注隐私保护和价值激励的一站式交互网络。Growchain 将面对全球市场推出多语言版本和多平台支持。

Growchain 依托于庞大的用户群体的多样化需求，以及由每一个参与者共同完善的母婴行业大数据的共享与脱敏，面向全球优质母婴品牌、应用开发者开放接入权限，并提供智能合约服务。在 Growchain 上，一切价值的转移都可以通过代币 Grow Token（简称：GROW）来实现。



二、项目背景

2.1 母婴市场概况

我们通常将定位于 0-6 岁年龄段婴幼儿使用的产品和服务称为母婴市场。母婴市场的消费主体是拟为或初为父母的群体，其群体具备的特征决定了母婴市场的深度和广度。

母婴消费是全球发达国家和大部分发展中国家的主要民生消费，且投入的力度也越来越大，母婴人群具有长期高频消费需求。

据艾瑞数据报告分析显示，2017 年全球母婴市场规模已破 2.5 万亿美元，预计未来每年将保持 10% 的增长率，2020 年全球母婴市场规模将突破 3.3 万亿美元。

2.2 母婴市场的特征

（1）消费能力强

从女性怀孕阶段开始，一个家庭就进入了强消费期：母亲的保健品、防护服、孕妇装、护理用品等；婴儿的奶瓶、童车、童装、专用洗涤用品、玩具等；同时还包括胎教、家政服务、幼教服务，以及家庭买房、换房，儿童入学等多种需求，婴儿的降生也伴随着刚性消费的支出。

（2）信息需求旺盛

由于普遍缺乏育儿知识，又对育儿的要求较高，准妈妈从怀孕初期就会产生迫切的信息需求，包括如何调整饮食和生活结构，如何胎教，如何预防小儿疾病，以及复杂的育儿技巧等。另外该群体有极强的交流分享需求。新妈妈有足够的时间乐于分享孕期、育儿经验。因此，同类群体的交流平台也是极其必要的。

2.3 母婴市场痛点

高速增长的母婴市场，也暴露出一些中心化的问题：

（1）寡头集中掌握着大量有价值的用户信息和行业数据，这些信息和数据的获取成本极高，在第三方介入后，同样存在造假的可能。

（2）用户在网上通过浏览点击、录入个人资料、交易商品等行为输出了大量有价值的个性化信息，既无法保证个人隐私受到妥善的保护，又不能得到收益。

（3）育儿市场版权意识薄弱，导致优质的内容创作者大量流失，劣质和陈旧的内容开始充斥于母婴行业。

（4）不透明的母婴产品生产模式，导致母婴产品存在极大的安全隐患，市场的信任严重缺失。

（5）具备品牌强背书的产品占据大量的市场份额，获得定价权，同类产品价格参差不齐。中小型品牌及应用具备优质的创意、质量和优惠的价格，但是在充满竞争的市场环境中不具备生存能力。

2.4 基于商业化公链的解决方案

2009 年中本聪创造比特币 [1]，宣告了第一代公有链的诞生。随后，以太坊 [2] 以其在商业应用方面的优势成为了第二代公有链的代表。随着区块链的不断发展，第三代区块链正在技术和应用的革新中显露出雏形。

在公链上做项目落地分为两种，一种是基于技术上的落地，作为公链吸引开发者在上面进行智能合约的开发以及 dapp 的落地开发，比如 ETH、EOS；另一种落地是基于某种领域的商业应用落地，垂直化是一个很好的方向。

我们惊喜的看到，在一个拥有中心化行业痛点的领域，一个垂直的商业化公链在精准交互方面具备了先天的优势。Growchain 作为一个围绕母婴行业生态逐渐扩张的区块链网络，使接入其中的用户、品牌和应用直接具备了商业上的内在联系，避免了无效的节点，同时直接摒弃了与行业无关的数据，使 Growchain 本身成为了一个不断完善的母婴行业大数据账本。

2.5 Growchain 的愿景

Growchain 将基于底层技术的不断完善，逐渐满足母婴行业涉及的各类商业应用场景的实现，在应用端为全球母婴用户提供一个满足成长记录、成长教育、母婴社交娱乐、母婴产品交易以及围绕未来更多创新需求等一切功能的一站式母婴平台。

我们将继续针对母婴行业存在的市场痛点，提出一系列基于区块链技术的解决方案，并通过创造更优的母婴行业生态体验，突破原本受到限制的用户需求，以刺激更创新、更有趣的需求的产生，推动全球母婴市场朝着更加健康的方向高速发展。

三、Growchain 的技术构架

当前区块链技术和生态已具有相当规模，但是实际落地的使用场景还比较少，Growchain 作为一个母婴行业 + 物联网的垂直化公有链，需要实现以下目标：

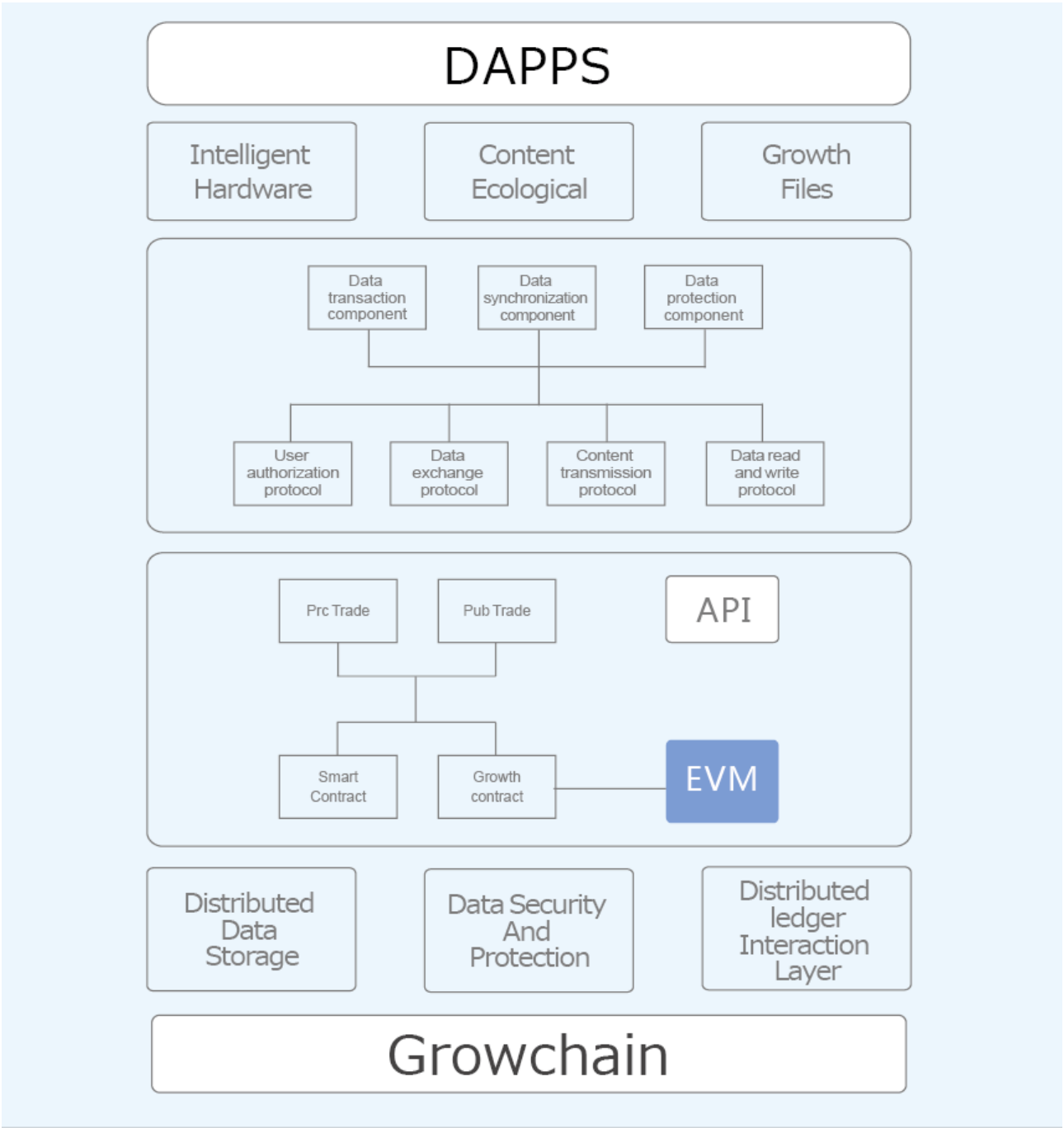
1. 用户数据的安全性
2. 用户数据的可交易及数据的流通性
3. 虚拟版权认证
4. 大量虚拟内容存储

基于上述目标，我们重新设计了 Growchain 的核心底层交互模块及关键部分数据结构：

1. 链的底层交互架构
2. 外部拥有账户的数据结构
3. 去中心化大型数据存储网络模块

我们选择主要使用 Growchain 的智能合约及去中心化数据存储服务为用户提供基于商业目标的服务。因为相对于现实世界，区块链世界的“行踪”更为清晰和可信：链上的交易数据忠实地记录了用户之间的每笔转账、以及每次对“智能合约”的调用情况。

接下来我们设计 Growchain 的基本框架，基于以上需求，Growchain 的数据层及协议层架构如下图所示：



为了实现以上基于实际需求的框架，Growchain 将会同时包含：

1. 以比特币为代表的链上指令概念的脚本

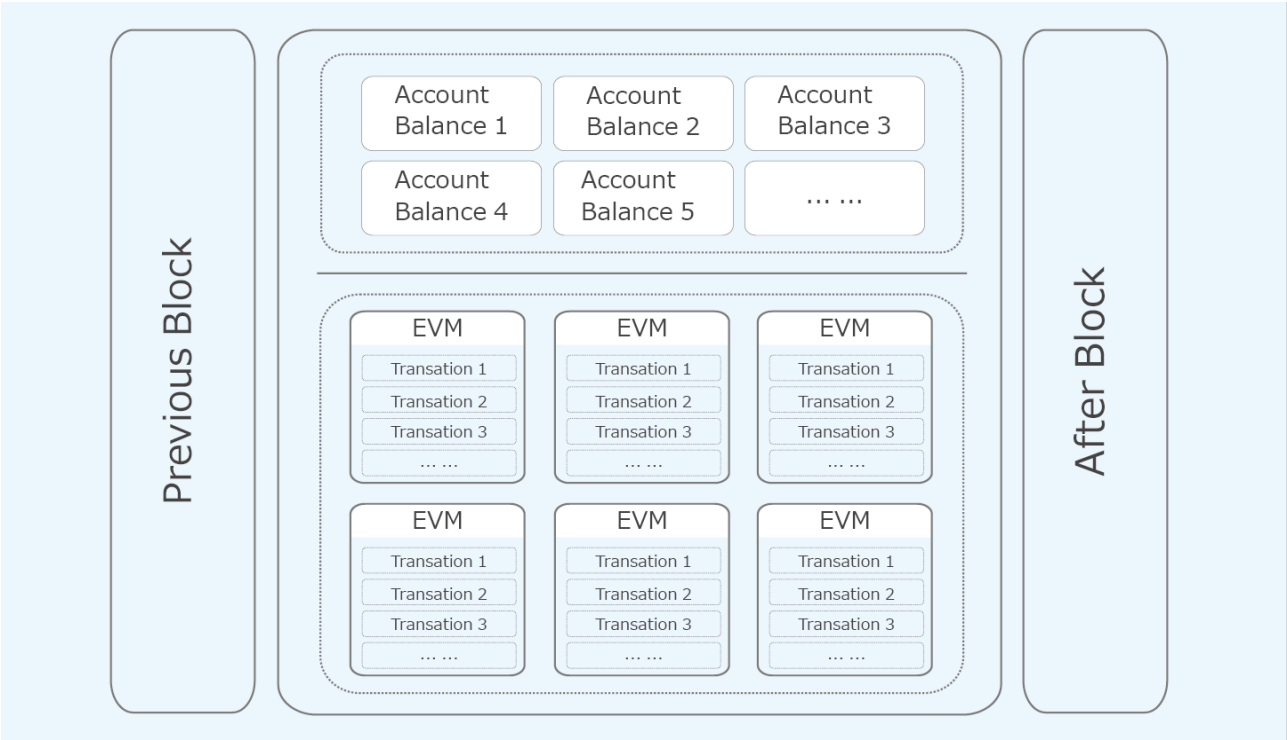
2. 以太坊为代表的链上智能合约功能

以此具备每个外部账户拥有必要数据时链上同步的相关处理能力。同时 Growchain 也将对智能合约的模型进行额外扩充，以满足母婴行业垂直化领域的商业需求。

3.1Growchain 主链结构

Growchain 的目标是以记录婴幼儿成长档案为基础，提供一个安全、可靠、去信任化的服务平台。基于此基础，Growchain 需要做到在记录必要的数据时链上自动同步而不需要手动操作（同样不需要矿工费），而在进行交易、转账等操作时需要收取一定矿工费，因此 Growchain 的主链将会包含链上指令及智能合约。

Growchain 的主链运行如下图所示：



基于以上需求和模式，Growchain 的外部拥有账户的存储结构将进行重新设计，除传统的账户地址、余额等数据外，Growchain 的外部拥有账户将为虚拟商品的版权使用、电商平台的使用、用户数据的存储等进行合理的结构保存。并且外部拥有账户除账户地址外其余数据都可由用户自行控制监视权限，以此确保用户数据的安全性及所有权。Growchain 的外部用户信息结构将添加如下内容：

```
public class User // 用户
{
     public UInt256  address  // 账户地址
     public ulong balance  // 账户余额
     ....  // 传统智能合约公链的用户数据
     public class Data  // 用户交互过的合约数据记录
     {
          public unit authority  // 权限
          UserChoose UInt256 targetAddress // 交互的合约地址
          UserChoose unit count // 与此合约交互的次数记录
     }
     public Data[] userDatas // 用户的全部合约交互记录
}
```

在 Growchain 的外部拥有账户的数据结构中，提供了 UserChoose 属性的数据结构，UserChoose 属性为用户所选择的隐私权限，对应等级权限如下：

1 表示 private 则不对外公开

2 表示 public 则对外部进行公开

3 表示 protected 则仅对此交易的合约进行公开。

Growchain 的所有用户数据将通过底层链上的指令在出现新区块时自动广播到链上网络，以确保链上可以及时的进行数据变更并永久存储用户数据。Growchain 约每 15 秒生成一个区块。新区块附加于前一个区块之后，形成一

个链式结构。每个区块内包含了 15 秒内网络内产生的全部交易信息 ,以及其他必要的检索和校验信息。

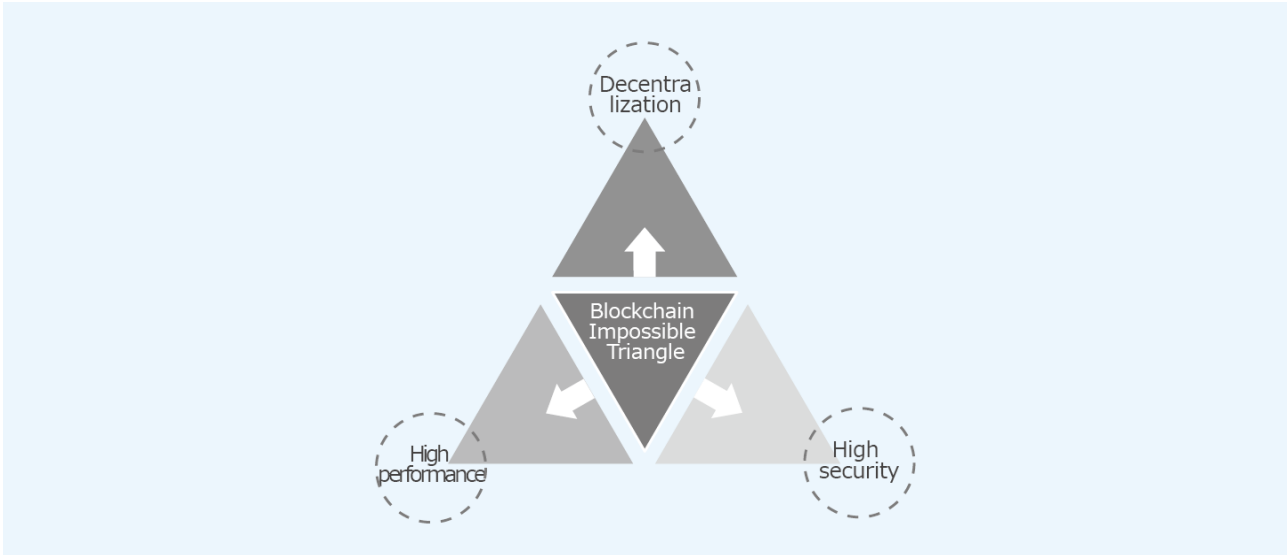
Growchain 的区块数据结构如下图示：

```
public class Block // 区块
{
      public uint Version; // 版本 public
      UInt256 PrevBlock; // 链接的区块
      public UInt256 MerkleRoot; // 交易列表的散列值
      public uint Timestamp; // 时间戳
      public uint Bits; // 保留字段
      public ulong Nonce; // 随机数
      public UInt160 NextMiner; // 下一个区块的记账人
      public byte[] Script; // 签名
      public Transaction[] Transactions; // 交易列表
}
```

Growchain 包含了自创世块以来的所有交易信息，依次执行这些交易就能得到当前的所有资产的归属和状态。区块链技术的去中心化特点保障了系统的稳定性和安全性；公开数据特点保证了系统的透明性和可追溯性；Growchain 可以以极低的成本完成传统中心化数据库的等量事务。

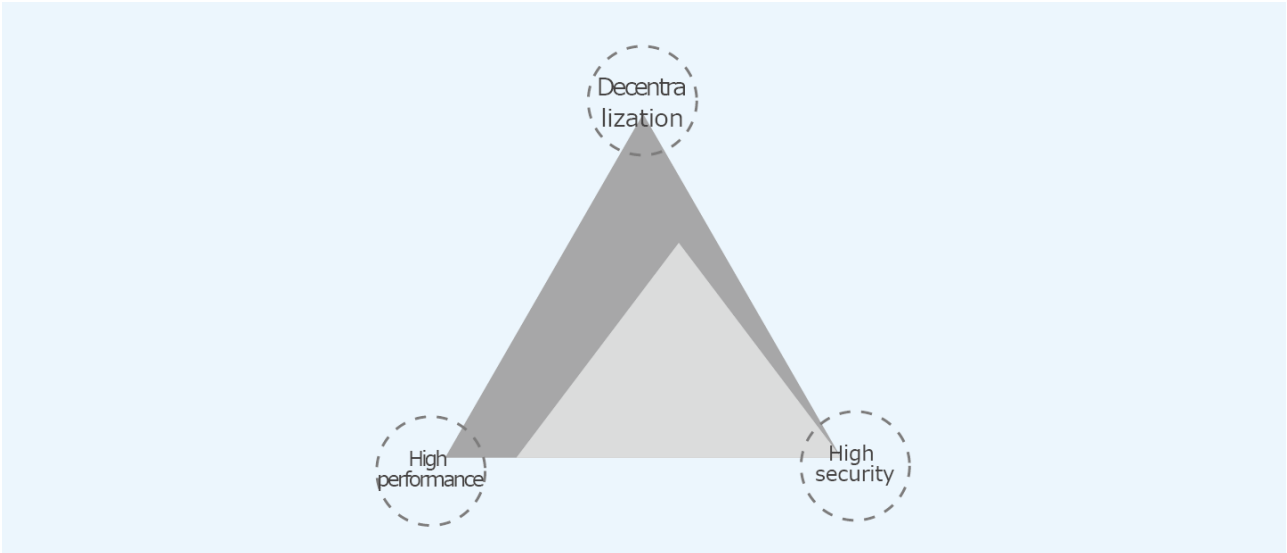
3.2Growchain 基于商业化公有链的取舍及优化

在区块链领域，有个不可能三角[12]，即不可能同时兼备：安全性、去中心化、高性能。



为了保证去中心化和安全性，比特币牺牲了性能 (7 TPS)。目前以太坊的设计基本与 BTC 差不多，所以，在性能方面根本无法支撑大规模的 DAPP 应用。EOS 重点提高性能以加强可扩展性，但他的多线程处理方案极大程度的牺牲了去中心化。

Growchain 基于商业化的需求对不可能三角进行了取舍，如下图所示：



Growchain 会将用户的安全性放在第一位，并且 Growchain 认为基于商业化的公链一定不是完全去中心化的，将会是多中心或是弱中心化，所以在一定程度上牺牲去中心化属性，而对于 Growchian 的性能将会继续使用算法进行优化，相对于 PageRank[8][9] 和 NCDawareRank[7] 等排名算法，在大交易量的情况下，算法优化模型如下：

$$S = x_1, x_2, \ldots, x_n$$

$$x_i \in \sum$$

表示一个长度为 N 的交易数据流。其中，$\sum$ 表示一个包含 n 个字符的符号表。我们用 $fs(x)$ 表示字符 x 在 S 的出现次数。我们给定一个常数 $0 < \phi < 0.5$，找到所有在 S 中出现了至少 ϕN 次的字符，即

$$I(S,\phi) = \{x \in \sum | fs(x) \geq \phi N\}$$

易知：

$$|I(S,\phi)| \leq 1/\phi$$

否则 $I(S,\phi)$ 中的字符在 S 中将出现大于 $\phi N \cdot 1/\phi = N$ 次。

我们假设：

$$N >> n >> 1/\phi$$

另外，我们也假设：S 中的字符按照顺序依次到来。因为区块的内存空间有限，我们无法将 S 保存下来。所以提供了一个只需要 $O(1/\phi)$ 空间的算法，而且可以保证算法得到的结果

$$I^+(S,\phi)$$

满足：

$$I(S,\phi) \subseteq I^+(S,\phi)$$

该算法维护了 $1/\phi$ 个计数器(占用 $O(1/\phi)$ 的空间),均初始化为 0。在算法中，我们将把空闲的计数器（即计数显示为 0）赋给新到来的没有计数器的字符。当 x_i 到达的时候，有三种情况：

1、如果 x_i 有计数器，其对应的计数器加 1；

2、如果 x_i 没有计数器，但存在着空闲计数器（计数为 0），那么就把这个计数器赋给 x_i，计数更新为 1；

3、如果前面两种情况都不成立，那么所有计数器都减少 1。

当 S 所有元素都已到达并处理完时，返回所有计数器的当前所有者，记作：

$$I^+(S,\phi)$$

这里，我们证明

$$I(S,\phi) \subseteq I^+(S,\phi)$$

假设

$$x \notin I^+(S,\phi)$$

那么在算法中，x 一共被消去了 $fs(x)$ 次。这里的消去是指：

1、x 到来的时候正好属于上面提到的第三种情况；

2、x 所持有的计数器因为其他字符的到来而减 1。

无论是哪一种情况，每次 x 被消去的时候，同时也有其他至少 $1/\phi$ 个字符被消去。因此，总的消去的字符至少为

$$fs(x)(1/\phi+1) \le N$$

因此

$$fs(x) < \phi N \Rightarrow x \notin I(S,\phi)$$

如果我们允许读取多一遍 S，那么我们可以精确求出 ϕ

$$I(S,\phi)$$

即在固定的区块大小下可以最优解决交易处理速度的问题。

3.3Growchain 的签名抽象

基本上所有的虚拟货币都是使用 256 位 ECDSA 签名来保障安全，但如果两次 ECDSA 签名使用相同的随机数，私钥就会被泄漏；虽然客户端程序会避免这种情况出现，但无疑说明没有任何一种签名算法是绝对安全的；所以抽象的签名层无疑让 Growchain 的安全性可以随时升级。

(1) 将支持的签名和加密算法 [19]

secp256k1 曲线 [16][17] 是 ECDSA 中经典和安全的曲线，也是绝大多数加密货币选用的曲线，所以 Growchain 的加密和签名默认选择 secp256k1 曲线。sm2[18] 是国家签名法指定的加密方式，所以 Growchain 也支持 sm2 签名，曲线选用 Fp256，而 sm2 使用的哈希算法将使用国密 sm3。

(2)Growchain 上的签名格式如下：

```
signature
{
    uint8 signType;
    uint8 v;
    uint256 r;
    uint256 s;
}
```

通过 signType 的不同值来标示签名算法类型。signType 空间将可以支持最多 256 种算法，甚至可以一定程度上防止量子计算机的攻击。

3.4Growchain 智能合约和成长空间

Growchain 支持图灵完备的编程语言，Growchain 对链上的任何一个智能合约进行全周期、全方位的服务，对智能合约的发起、审核、部署、应用、清理等流程进行可控化管理，并对智能合约的各项操作进行实时安全监测。

3.4.1 Growchain 的智能合约

根据 Growchain 的业务需求，Growchain 提供的智能合约相对于现有的以太坊智能合约进行了创新，增加了以外部拥有账户内容及权限属性作为合约交换内容的全新合约模式，增加的合约模式可有效提升合约创建、订立、执行等各个环节的效率。同时，新的合约模式的生命周期及交易流程也进行了相应的调整，以适配不同的业务需求。Growchain 全新的合约模式应用场景稍后将会进行举例介绍。

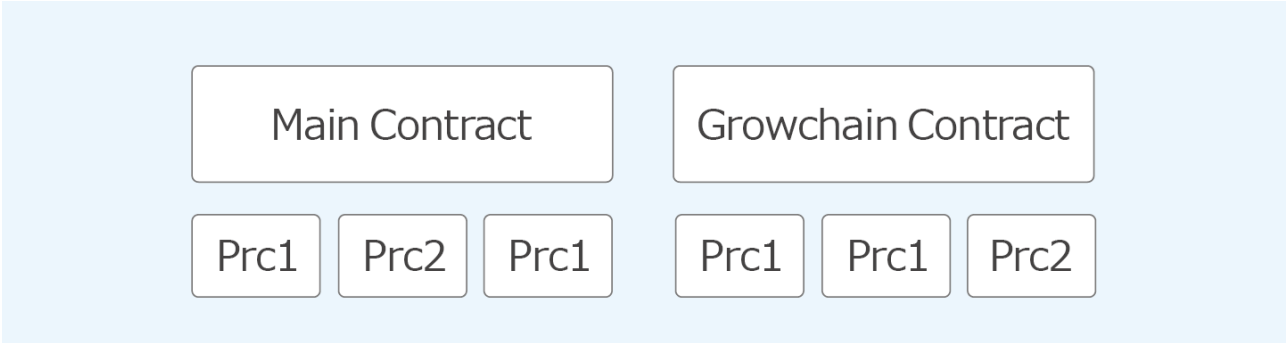
3.4.2 Growchain 的成长合约

用户与用户间通过私钥对智能合约进行签名，从而完成数字资产的转让交易，如果合约的标的物是登记在成长链上的区块链版权或数字资产，那么成长链可以自动在链上进行程序化交割执行；如果合同标的物为链外资产，那么合同参与方自行执行即可。即便是后者情况下，成长链也消除了签署、保管大量纸质合同的繁琐性，并用数字签名保证了合约的不可抵赖性。

Growchain 的合约分为智能合约(Smart Contract)和成长合约（GrowContract）。

成长合约（ Grow Contract）在智能合约的基础上，还将引入在母婴行业中符合各类业务逻辑和商业逻辑的区块链合约。例如交易合约，数据服务合约，激励合约，防伪合约等。还将兼容 EVM，EVM2.0，Lua，等更多的虚拟机类型。我们将发布基于 Javascript 的合约编程语言。Growchain 系统可以通过智能合约和成长合约管理合约参与者的身份，为基于 Growchain 系统的金融服务提供更好的支持。

3.4.3 Growchain 的智能合约架构



Growchain 的智能合约架构为基础智能合约与成长合约处于同一执行等级[20]，智能合约与成长合约都可以由用户自由创建多个具体交易的子合约，子合约的权限等级分为 private 和 public。

Private Contract 是生成的一个具体交易合约，适用于 1 对 1 的交易模式，PrC 合约不具备很好的流动性，但支持 P2P 的个性化合约签订。

Public Contract 也是生成的一个具体交易合约，适用于 N 对 N 的交易模式，PuC 具备良好的流动性。

Growchain 智能合约的具体事例

(1) 真正的实现用户的数据用户做主，并且用户的数据可以自主的进行变现，商家也可以通过此种智能合约主动获得一手用户数据，用户数据不再被大数据龙头企业垄断。比如：商家发布一个使用 Growchain 代币换取用户数据的智能合约，用户只需同意合约内容，就可以将自己想要公开给商家的数据换取代币，且用户的数据所有权还在用户手中，商家也可以进行一次性（或持久化，根据商家合约内容而定）的获取一手用户数据。

(2) 实现区块链物联网 ToC 端用户落地的最后一步时，即商家通过区块链网络进行商品销售的活动时，商家只需在链上创建出售商品的智能合约，以商品名称换取 Growchain 代币，买家用户同意合约内容后，商家进行发货，然后将快递单号传入对应的智能合约，并且可以选择用户使用私钥进行货物接收以避免误签收等情况，以此完成链上的电商交易。

3.5DPOS 共识机制

目前主流共识机制为 POW[3]、POS[4]、DPOS[10][11]、BFTP 等。现阶段 Peercoin[5] 和 Ethereum[2] 的 Casper[3] 协议都采用了 PoS[13] 共识算法。Growchain 将采用 DPOS[10]（Delegated Proof of Stake）共识机制，即股份授权证明机制（又称受托人机制）——由每一个持有 Growtoken 的节点进行投票，产生基于当前网络规模的一定数量的共识节点依次轮流进行记账（挖矿），这些共识节点彼此拥有完全相等的权利。作为最核心的节点排名指标，是过去几十年网络科学领域研究最多的一个概念 [6]。若共识节点在任何规定时间内不能履行其职责，便会被移除，系统会再次发起投票选出新的共识节点来代替。

DPOS[11] 算法分为两部分：选择一组块生产者和调度生产。即使用信誉系统以及无摩擦、实时投票的机制，来创造出一个有限信任的团体。团体中的参与成员有权利创造区块，将其加入区块链并禁止非受信的参与方加入其中。这些受信任的参与方通过随机分配的方式决定创造区块，并且每一轮还会被改变。因为见证人位置的数量是有限的（一般是奇数个），所以见证人会互相竞争来获得记账的工作。如果见证人主动降低他们获得的收入，那么他们就可以吸引到更多人的投票，同样，保护网络安全的费用将通过见证人之间的竞争维持到一个合理的水平。同时，恶意的见证人将会因为自己的作恶行为被快速投票出局。DPOS 共识机制可以有效避免对 Growchain 生态发展无益的节点，且无需消耗多余算力即可完成权益分配。

3.6 代币激励

Growchain 作为商业化公有链，必须通过代币（GROW）激励的经济手段形成共识——Growchain 上的每一笔交易的产生会同时消耗一定数量的代币作为对共识节点打包交易数据的激励。同时，为促进 Growchain 前期的快速发展，会向项目初期，每一个加入 Growchain 并通过信息核实认证的用户、优质应用或品牌提供一定的代币奖励。持有代币不仅可以获得发布智能合约等区块链基础服务，还能成为权益节点，参与投票。

GROW 代币激励的引入会使节点维护者在维护账本的安全性与真实性的同是能够得到代币奖励，优秀的智能合约编写者也能够得到代币激励，而作恶者由于接入智能合约需要一定的手续费使其成本大大增加，对 Growchain 进行攻击所窃取的代币会由于其举动对区块链造成的打击而价值大大降低。

3.7 开放应用接口

为了使商家能够在 Growchain 上快速接入自己的应用，Growchain 提供多语言的一系列底层数据访问和交互接口，同时支持多语言集成和功能扩展。

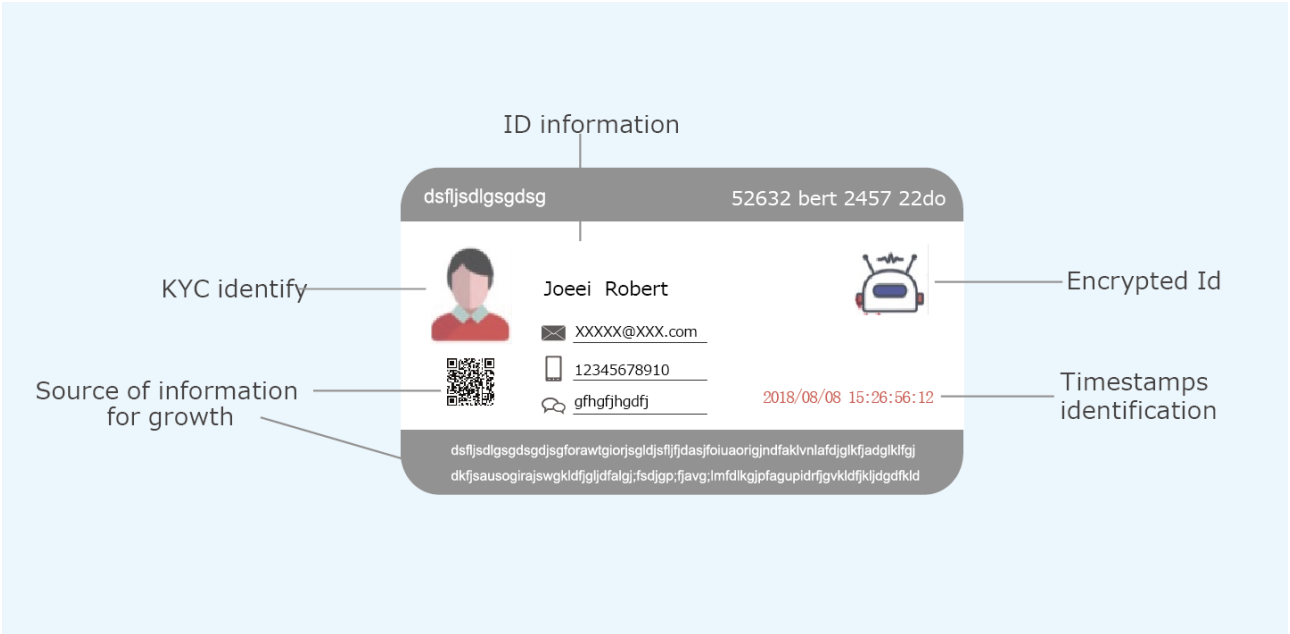
四、Growchain 的应用场景

Growchain 作为一个垂直市场的商业化公链，依赖于区块链技术去中心、去信任、匿名性、不可篡改等特点，将提供一系列围绕母婴的创新应用：

4.1 数字成长档案

用户可以在孩子出生后，通过 Growchain，为孩子建立数字身份证，该身份证经过加密确认和独一无二的时间戳证明，将成为一个永远不会被篡改或丢失的数字成长档案的开始，并且随着时间的推移和孩子的成长，用户在 Growchain 上产生的每一个数据，比如听了某一首童谣、喝了某个品牌的奶粉，都会被记录在这个成长档案中，而且可以随时查看。

在 Growchain 上，任何人和机构都可以基于智能合约，完成和用户数据，用户交互相关的交易。例如用户消费偏好数据可能是各方构建自己算法的核心，基于一个约定的合约，用户可以选择性开放自己的某些数据维度，而这些数据的开放可以使得用户获取相关应用的奖励及代币等，而数据所有权属于用户。



Growchain 还将围绕档案数据的全生命周期进行管理，采取分布式认证、分片存储、快速共享、安全管控等技术手段，覆盖档案的归档、保存、调用、共享、移交、销毁等环节，促进档案管理的安全体系和共享机制建设。

具备如下特点：

a、仿伪造：建立分布式数字认证机制，防止档案内容被篡改；

b、防黑客攻击：档案认证信息进行分片存储，随机验证，使黑客无固定攻击目标；

c、简化档案调用流程：通过平台建立共享机制，简化调用流程；

d、可溯源：基于档案信息的共享交换记录，可查询任意时刻的档案管理业务行为；

e、可管控：对违规共享交换行为，可实施阻止和预警。

此外，在孩子入学方面，Growchain 已取得美国基础教育授权（包含 kindergarten、primary school、junior high school、high school ），即包括从 kindergarten 至 K12 的课程教育。通过线上教育区块链证明学分机制合作，孩子在家就可以读美国名校，使得参加美国 SAT 直升美国大学成为现实。

4.2 Growchain 的母婴内容生态

Growchain 将为母婴领域的内容创作者提供版权认证及作品溯源服务，包括但不限于视频版权、音乐版权、软件防伪、数字内容确权，软件作品溯源等，创作者从产生创意到输出均由 Growchain 进行记录，内容经审核和算法认证，生成不可篡改、公开可查的数字版权证明，彻底杜绝了盗版的产生。该证明可成为 Growchain 上内容交易的凭证，用户或商家均可以通过代币向内容创作者申请内容的打开权限或版权购买。

在 Growchain 上，作品一旦上传，便拥有区块链唯一认证数字签名，并自动进行全球版权声明，在世界范围内保护创意者知识产权。此外，Growchain 还建立了直接付费机制，实现电商平台忠诚度积分分配与赎回，基于智能合约的利益自动分配实时结算，无中间商无差价使交易完全透明化，真正实现了让利润回归给内容创造者。

除此之外，Growchain 还利用区块链的内容预定模型、时次售卖模型、分销商模型三种数字作品交易模式，丰富数字商品的获取和使用问题。在此过程中，依托社区化经营，Growchain 采用电商平台忠诚度积分分配与赎回机制，基于智能合约进行利益自动分配，实时结算，将利润回归到创作者手中，从根本上解决数字商品安全保护和交易信任。

4.3 智能硬件底层服务

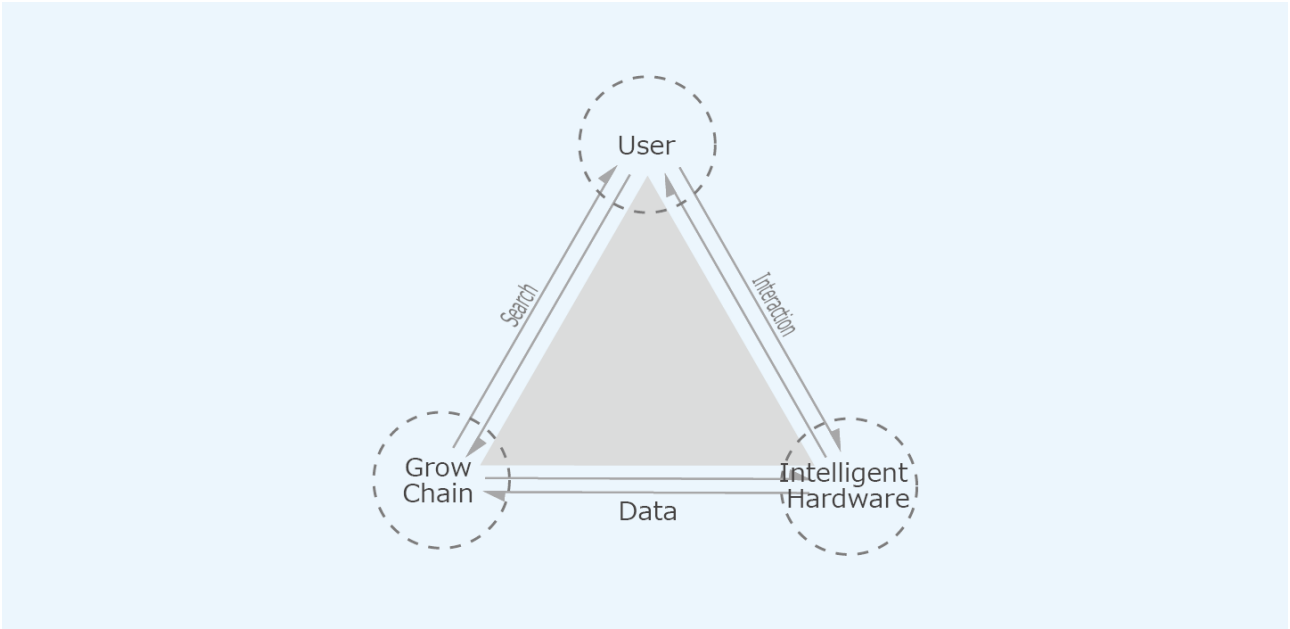
Growchain 支持母婴领域智能硬件及应用的接入，一方面，Growchain 可对大量的物联网 [14][15] 数据进行分布式存储，其中负责记账（挖矿）的代理节点会完成数据的处理和网络的共同维护；另一方面，垂直的母婴区块链网络对同样垂直的母婴行业智能硬件产品有着极佳的接纳性。

Growchain 为智能硬件提供点对点直接互联的方式进行数据传输，整个网络不需要引入大型数据中心进行数据同步和管理控制。Growchain 可以对智能硬件产品架构给出如下三方面的支持：

a、分布式数据传输和存储的构架；

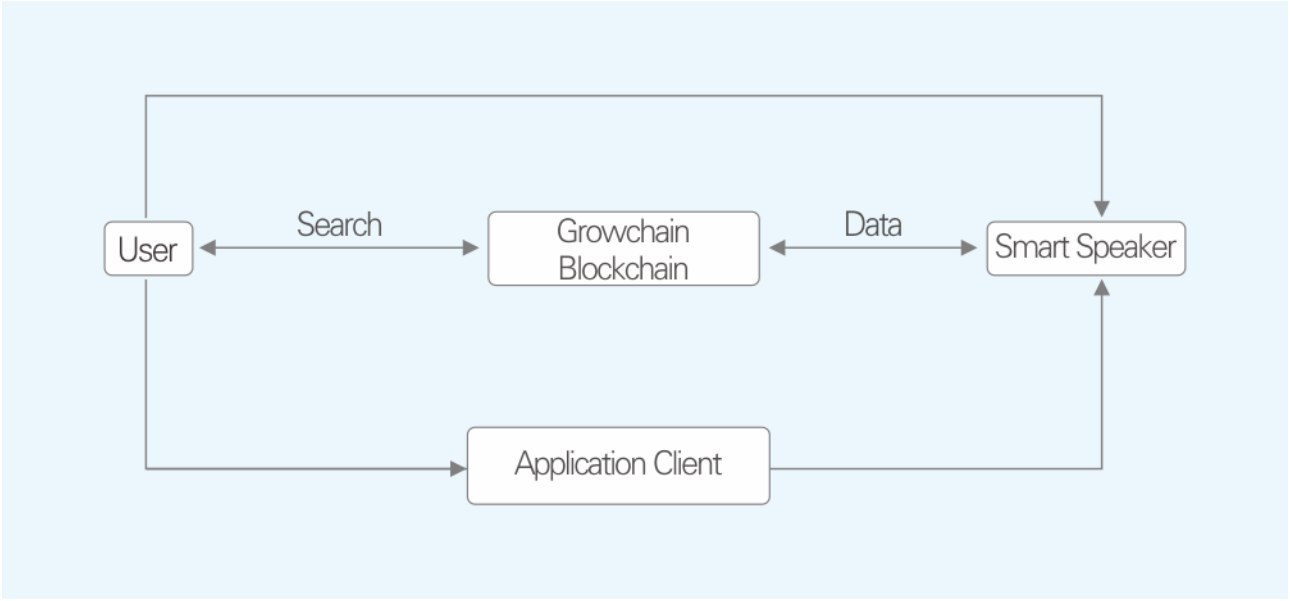
b、数据的加密保护和验证机制；

c、便捷稳定的费用结算和支付。



通过用户需求的反馈，基于区块链建立母婴行业智能硬件的全新商业模式，人们更加希望智能硬件能够在给定的规则逻辑下进行协助，完成各种具备商业价值的应用。Growchain 可用于构建智能硬件的分布式网络，连入其中的设备之间能够安全高效的交互和通信，并实现复杂的商业逻辑。

Growchain 通过对智能硬件提供底层服务，可以在实际应用中接入专门为母婴行业设计的智能音箱、智能手表等智能硬件产品。下面是智能音箱的具体实现架构。



4.4 Growchain 的社交功能

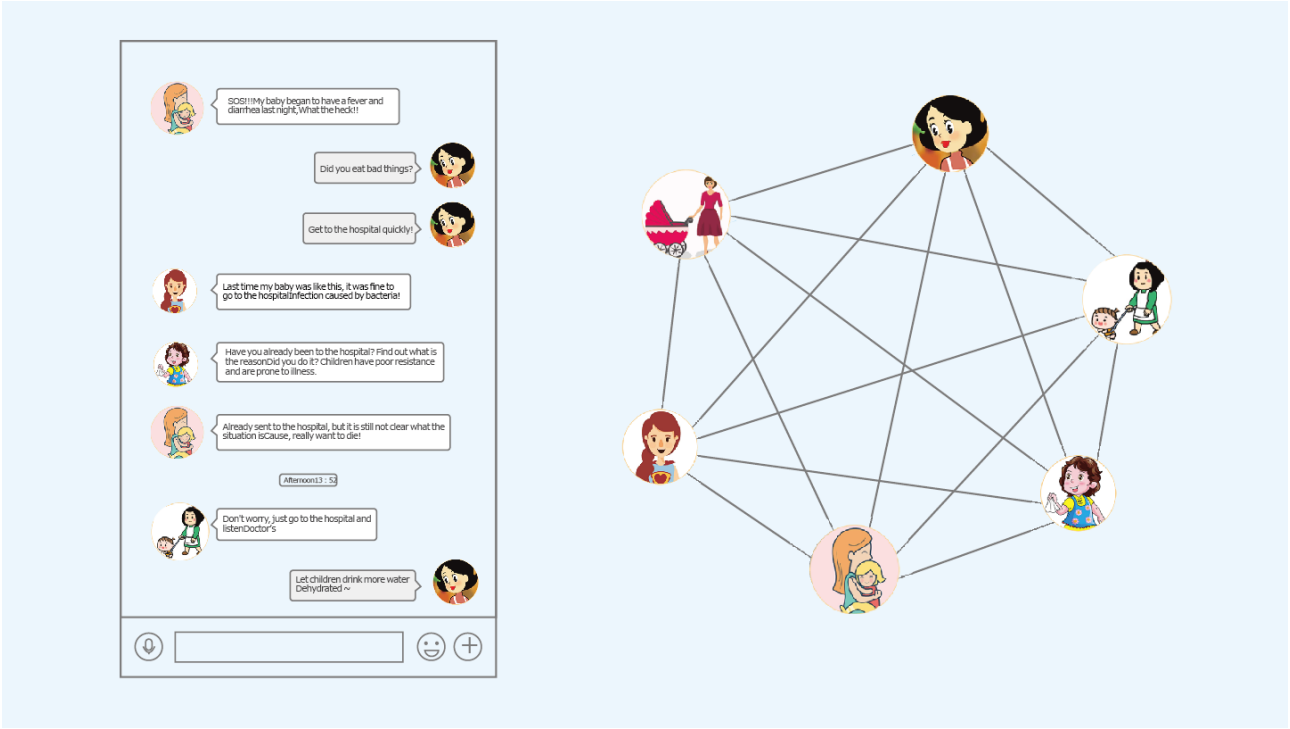
目前的社交网络是中心化的结构，由用户创造内容，由社交网站设定规则、存储内容、分发内容。用户之间的交互通过中心化的社交网络实现，利用社交网络进行人际关系的沟通与维护、获取朋友动态、热点内容等信息，而作为服务提供方的社交网络则掌握了用户产生的数据，并通过分析这些数据，进行精准的广告推荐，从而获益。

而 Growchain 社交的特点是：

（1）不记录和储存任何个人信息

（2）不向用户推送精准广告

Growchain 具备良好的匿名性和全网实时广播的特点，妈妈们可以通过孩子的数字身份证获得准入，以使用 Growchain 提供的社交功能——在互不公开个人身份信息的前提下，组成一个完全由妈妈构成的社交网络，可自由地进行日常晒娃、经验咨询、吐槽互动等全网共同参与的社交活动，并可通过悬赏代币的方式获得更为专业的咨询和辅导。



Growchain 社交网络允许用户在自己设备上运行节点接入网络，节点与节点之间实时互连，用户信息以加密形式存储在网络节点上，形成一个分布云。按照区块链技术，数据是冗余存储，数据只有掌握了秘钥的人才能查看。网络会向做出存储和算力贡献的用户提供补偿。此外，也会向创建和维护内容的用户提供奖励。

通过这样的方式，它建立了跟传统社交网络完全不同的运作模式：把用户资料和信息的控制权归还给个人，并为有贡献的用户提供激励。这样的模式一是保证了个人数据安全，二是通过系统机制刺激大家做更多的贡献。网络在这个时候，不再是中央枢纽，而是单纯的平台，一个用户完全可以点对点进行交互的平台。

五、Growchain 的经济系统

5.1 代币发行方案

GROW TOKEN（代码：GROW）总量 50 亿个，恒定不变。其中 40 亿个（总量 80%）一次性生成，10 亿个（总量 20%）伴随着每个新区块的生成而产生。

第一年（实际为 0-200 万个区块），每个区块新生成 80 个 GROW；第二年（实际为第 200-400 万个区块），每个区块新生成 70 个 GROW；以此类推，每年递减 10 个 GROW，直至第 8 年递减至每个区块新生成 10 个 GROW；自此保持每个区块新生成 10 个 GROW 直至约 22 年后的第 4400 万个区块，GROW 总量到达 50 亿，则停止伴随新区块生成 GROW。

按此发行曲线，第 1 年会有 83.2% 的 GROW 被创造，前 4 年会有 90.4% 的 GROW 被创造，前 12 年 96% 的 GROW 被创造。

5.2 代币分配方案

一次性生成的 GROW 分为两部分，第一部分 20 亿个用于按轮次和比例分发给 Growchain 开发经费众筹的支持者。

第二部分 20 亿个由 Growchain 基金会管理，用于支持 Growchain 网络的长期开发、运维和生态发展。该部分的 GROW 初始为锁定状态，在 Growchain 网络运行达半年时方可解锁被使用。这部分 GROW 不会进入交易所交易，仅用于长期支持 Growchain 项目，拟按如下比例分配使用：

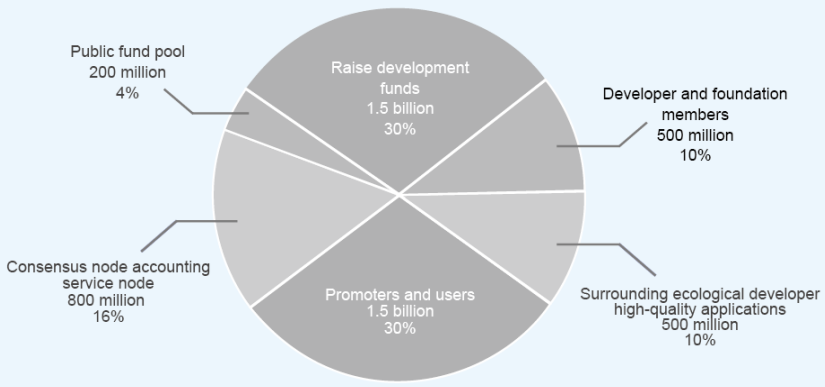
5 亿个（总量 10%）用于激励 Growchain 开发者和基金会成员。

5 亿个（总量 10%）用于激励 Growchain 周边生态开发者、优质应用、品牌。

10 亿个（总量 30%）用于激励 Growchain 推广者和使用者。

除用于激励 Growchain 推广者和使用者的 GROW 外，每年使用的 GROW 原则上不得超过 2 亿份。

伴随新区块生成而产生的 GROW，80% 作为激励奖励给提供共识结点记账服务的节点，20% 做为公益基金汇入由 Growchain 基金会管理的 Growchain 公益基金池。

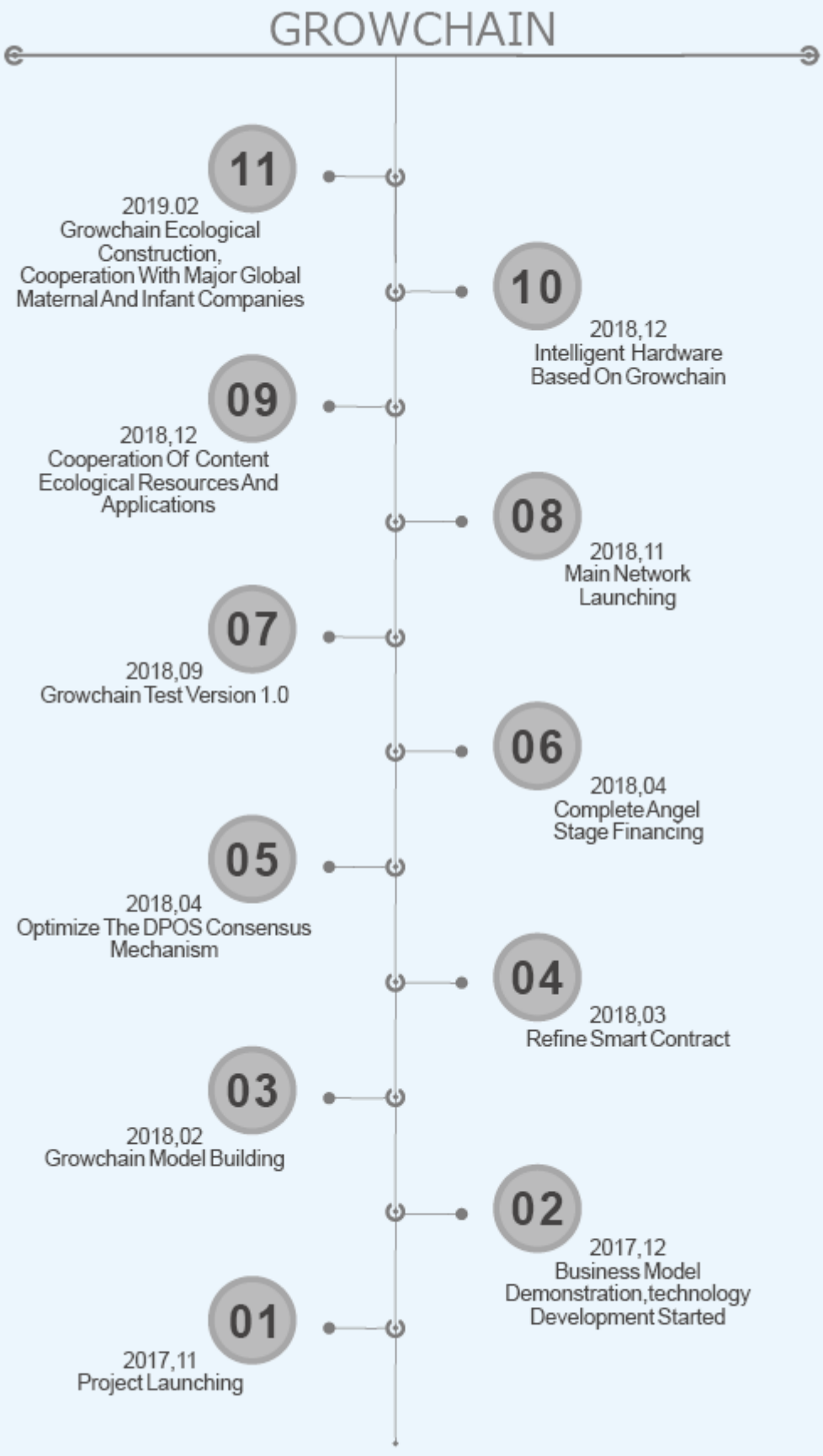


Growchain Distribution Map

5.3 募集资金分配

使用分类	比例	明细内容
技术开发	25%	初始技术开发团队的奖励，专家级开发人员的招募；专利及知识产权保护等一系列活动。
商业开发	50%	商业应用落地、项目扶持、商业拓展、 人员培训、项目交流与分享、刊物发表、社区创建和维护等。
市场与法律服务	10%	用于奖励为社区的推广运营做出共享者，以及提供法律服务等相关事宜的人员。
基金会运营	15%	基金会日常管理、交通、办公、财务、人力等需求及储备。

六、Growchain 的发展路线图



七、核心团队

核心成员

CEO Henry Schellhorn

克莱蒙特研究生大学（CGU）数学科学学院的数学副教授，德鲁克管理学院的金融工程项目学术主任，曾担任甲骨文公司的首席研究工程师，现担任《应用数学和决策》科学杂志的副主编，及其他一些著名金融、数学和运筹研究等方向的出版物的审稿人。

CTO Allon Percus

克莱尔蒙特研究生大学（CGU）数学科学研究所教授， 应用数学家，数学领域的前沿人物。开发了极值优化（Extremal Optimization）方法，领导了Los Alamos 国家实验室的多个跨学科项目团队并得到了空军科学研究办公室、国家科学基金会、能源部和南加州爱迪生等机构的资助。

COO Yi Feng

曾任 CGU 学术事务副主席，政治经济学系主任，专注领域是国际政治经济学、公共政策分析和定量方法论。在国际政治经济学、国际关系、区域一体化与全球化的政治经济学、公共政策研究、亚太政治经济学，量化研究方法和计算机应用数据分析等学科具备深厚的研究背景并任授课导师，曾任国际研究协会年会总计划主席，以及作为《国际互动》杂志的编辑。

CFO Thomas Willett

克莱蒙特研究生院经济科学系霍顿经济学教授、克莱蒙特·麦肯纳学院罗伯特经济与金融学院、克莱蒙特经济政策研究所所长，其研究专业包括国际货币经济学、行为金融学、政治经济学、国际金融危机和国内外经济政策分析等方向，曾在哈佛大学和康奈尔大学任教，曾担任总统经济顾问委员会的高级经济学家，美国财政部国际研究部主任，国际货币基金组织访问研究员。

Market Manager Issam A. Ghazzawi

勒芒大学的管理学教授和山姆·沃尔顿研究员，拥有超过 20 年的行政管理经验，曾在美国利盟、微软、联想美国、泰格斯等公司担任咨询顾问，此外，他还曾在加州圣贝纳迪诺 ITT 理工学院担任顾问，多伦多最大的合作集团安大略联合合作社（UCO）的董事会成员，Enactus 美国教师咨询委员会成员。

Asia Pacific Leader Rocky Hogan

南非金山大学商学院工商管理硕士，曾任职于花旗银行亚太区高级管理人员，负责花旗亚太区零售业务，具有丰富的市场经验

基石投资

朴素资本成立于 2015 年 7 月，总部位于深圳，在上海、香港、欧洲、美国设有分部。截至目前，朴素资本发起设立私募股权基金 20 余只，管理的基金规模超过 80 亿元，资产管理规模达 100 亿元。

大西部创投重点关注于教育、能源及资源、有机农业、互联网技术及应用、新媒体、医疗健康、先进制造等诸多领域的拥有一流品牌的领先企业，覆盖初创期、成长期、成熟期、Pre-IPO 各个阶段，投资规模从百万元到上亿元不等。

欧美区顾问

世界区块链组织（World Blockchain Organization）

简称为 WBO，联合国经济和社会事务署 (United Nations Department of Economic and Social Affairs) 注册的非政府组织。

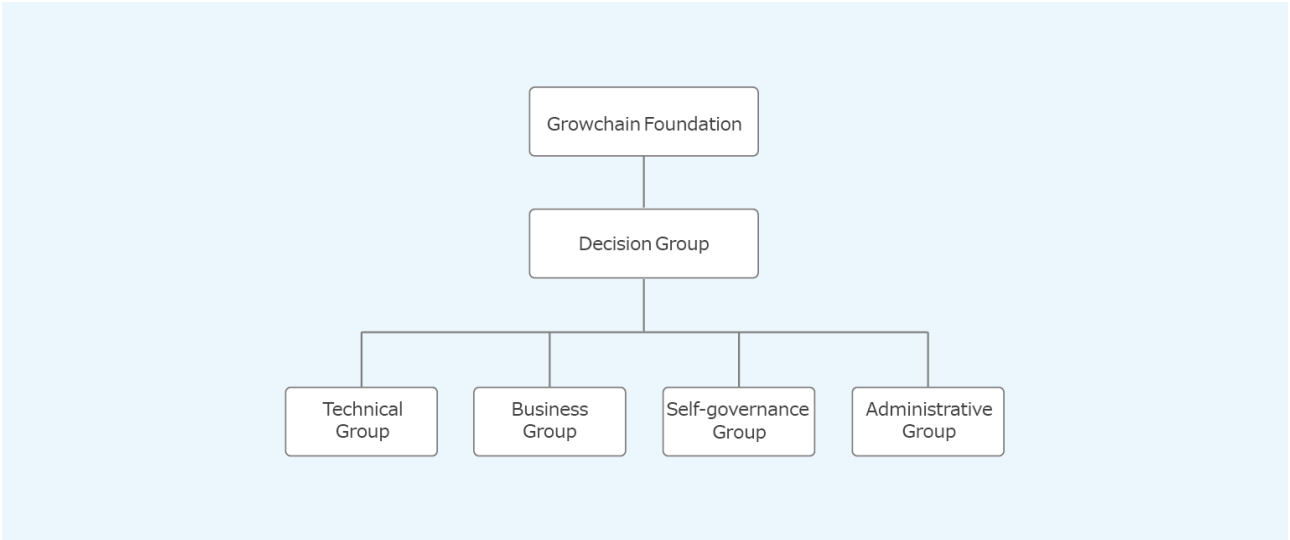
八、基金会与合作理事

8.1 Growchain 基金会

Growchain 基金会将致力于 Growchain 的建设、维护和推广工作，推进基于 Growchain 的母婴行业新生态的快速健康发展。

Growchain 基金会组织架构由决策组以及决策组下设的技术组、商务组、自治组和行政组构成，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。基金会成立初期，决策组由 Growchain 核心开发人员和运营成员组成，一共 7 人，任期为 3 年。

下一届决策组由社区根据代币持有量、活跃度及贡献等指标按不同权重计算，并投票选出 100 名社区代表，再进行投票选出新一届决策组成员。被选出的 Growchain 基金会各组成员均须保持高标准的信誉和商业道德；遵守相关的法律法规及行业自律原则；提供透明的财务管理；Growchain 将邀请国际知名第三方审计机构对 Growchain 基金会的资金使用、成本支出、利润分配等进行审计和评估。Growchain 将无保留的公开第三方机构的评估和审核结果。



8.2 合作理事

Growchain 基金会已与联合国世界区块链组织达成理事合作。

世界区块链组织（英语：World Blockchain Organization；简称 WBO；中文简称“世链组织”），是联合国经济和社会事务署（United Nations Department of Economic and Social Affairs）注册的非政府组织。

世界区块链组织由联合国项目服务办公 - 室（UNOPS）、联合国粮食计划署（WFP）、联合国开发计划署（UNDP）、联合国儿童基金会（UNICEF）、联合国妇女署、联合国难民署（UNHCR）和联合国发展集团（UNDG）倡议，世界自由贸易区联合会 (World Federation of Free Trade Zones)、加勒比自由贸易区（Caribbean Free Trade Zones）、加勒比区块链研究院（Caribbean Institute of Blockchain industry）、联合国可持续发展目标治理和竞争力国际组织（WOGC -- World Organization of Governance & Competitiveness for the UNSDGs）、关键会务 (Keynote Events) 联合发起。

Growchain 基金会将与联合国世界区块链组织共同鼓励和推动区块链的发展，共建区块链友好社会。

Word Blockchain Organization

TOWARDS A BRIGHT BLOCKCHAIN+FUTURE

九、风险声明

Growchain 作为一项在全球母婴行业和区块链技术方面的创新探索，将面临诸多政策、法律和市场的不确定性，对于投资人和 Growchain 平台，这种不确定性既是一种需要极力规避的风险，又意味着抢占先机便能掌握优势的机遇。

9.1 合规、运营性风险

合规、运营性风险是指 Growchain 公有链在募集资金以及开展业务过程中违反当地法律，造成经营无法继续的风险。Growchain 是一个国际化项目，服务面向全球市场，将会面临各个国家和地区对数字资产交易及 ICO 监管政策的不一致。据统计，在全球受统计的 246 个国家中，有 40%对数字资产交易和使用不加限制，有 3%是受限市场，4%将其定义为非法，其余占比 53%仍没有更多对待数字资产的相关信息。

针对该风险，Growchain 的法律顾问团队会密切关注各国政策，拥抱监管，并根据相关条例提前布局。在开展业务的当地聘请专业律师，在法律框架下设计相关业务，同时，为满足和遵守当地法律法规，Growchain 平台可能会在有些地区无法提供正常的服务。

9.2 市场风险

市场风险是指 Growchain 没有被市场接纳或没有足够用户使用造成业务发展停滞和利润支撑的风险。

针对该风险，Growchain 团队经过在母婴产品领域丰富的市场运行经验，确认了市场痛点的客观存在。利用团队在母婴、物联网领域中积累的经验以及更多金融及区块链方面人才和顾问的引入，迅速孵化平台生态并产生利润。

9.3 技术风险

技术风险是指 Growchain 的底层技术出现重大问题，导致 Growchain 公链无法实现与其功能，以及关键资料被篡改或丢失的风险。

针对该风险，Growchain 聘用了成熟的区块链开发团队，基于成熟、开源的区块链技术，采用已经被用户认可和验证的构架开发和完善 Growchain 公有链系统。

9.4 资金风险

资金风险是指项目资金出现重大损失，例如：资金被盗、资金亏损、储备金贬值等风险。

针对该风险，Growchain 采取多重签名钱包 + 冷存储的方式，并由基金会掌管。运营团队具备着丰富的金融行业服务经验和风控经验，流动资金在市场上的波动超过 50%才会出现亏损的可能。

十、补充说明

除本白皮书明确规定的情况外，我方不会就 GROW 代币作出任何声明或保证。每位参与方获得任何 GROW 代币，应按照本文中披露的信息对 GROW 代币进行操作。

无责任

本基金会特此声明对下列情况不承担任何责任：

（1）任何人违反管辖区域的洗钱、恐怖融资或其他监管要求的；

（2）任何人违反本计划下的任何陈述、保证、义务、契约或其他规定参与活动，以及由此导致的失败和无法检索其付款或索取购买的 GROW 代币；

（3）Growchain 平台开发失败或退出，导致未能向购买者交付 GROW 代币；

（4）推迟或重新安排 Growchain 平台开发，导致未能达到任何预期的里程碑；

（5）Growchain 平台源代码的任何错误、缺陷或其他错误；

（6）启动后的 Growchain 平台的任何故障、崩溃、回滚或硬分叉；

（7）Growchain 平台或 GROW 代币未能达到任何特定目的或不适合任何特定用途；

（8）未能实时全面披露有关 Grow 平台的任何信息；

（9）任何参与方泄露、丢失或破坏他 / 她的 GROW 钱包的私钥；

（10）GROW 代币被任何政府、准政府、权力机构或公共机构分类或视为某种货币、证券、商业票据、可转让票据、投资或其他可能被禁止、管制或受某些法律限制的条款；

（11）在任何加密资产兑换中列出或退出 GROW 代币；

（12）任何人流通 GROW 代币；

（13）Growchain 平台上的任何应用程序、智能合同或其他程序；

（14）本计划中披露的任何风险因素，以与该风险因素有关的任何损害、损失、索赔、责任、惩罚、成本或其他不利影响。

税款

参与方应声明， 承担和支付任何管辖区的法律和法规由于持有、使用、购买、收购 GROW 代币所应支付的税款，并且每个参与方应对其不付款、少付款、不正当的付款或逾期支付任何适用税款的所有罚款、索赔、惩罚、责任或其他方式负全部责任。本计划对任何买方的税务意图不作任何建议，也不作任何陈述。

没有豁免

本计划未能要求或强制参与方严格遵守的任何条款，或本计划未行使本协议的权利，不得解释为放弃本计划的权利或依赖任何此类条款或权利的权利。关于对本计划的任何规定条件或要求的明示放弃，不构成对将来有义务遵守该规定的条件或规定的放弃。

可分割性

如果本计划的任何部分（无论是全部还是部分），根据任何管辖区的法律为非法或无效，不得影响该管辖区其他计划的合法性或有效性，也不影响在任何其他管辖区的计划的合法性或有效性。

十一、参考文献

[1] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System." In: Www. Bitcoin.Org(2008), p. 9. issn: 09254560. doi: 10.1007/s10838-008-9062-0. arXiv: 43543534534v343453.url: https://bitcoin.org/bitcoin.pdf.

[2] Vitalik Buterin. "Ethereum: A next-generation smart contract and decentralized application platform." In: URL https://github. com/ethereum/wiki/wiki/% 5BEnglish% 5D-WhitePaper(2014).

[3]Vitalik Buterin et al. Ethereum white paper. 2013

[4]The Stage 1 Casper Contract. https://github.com/ethereum/casper/. Accessed: 2017-08-01

[5]S King and S Nadal. "Peercoin–Secure & Sustainable Cryptocoin." In: Aug-2012 [Online]. Available: https://peercoin.net/whitepaper ().

[6]Mark Newman. Networks: an introduction. Oxford university press, 2010.

[7]Athanasios N. Nikolakopoulos and John D. Garofalakis. "NCDawareRank." In: Proceedings of the sixth ACM international conference on Web search and data mining - WSDM '13 February 2013 (2013), p. 143. doi: 10.1145/2433396.2433415. url: http://dl.acm.org/citation.cfm?doid=2433396.2433415

[8]Sergey Brin and Lawrence Page. "Reprint of: The anatomy of a large-scale hypertextual web search engine." In: Computer Networks 56.18 (2012), pp. 3825–3833. issn: 13891286.

[9]Lawrence Page et al. The PageRank citation ranking: Bringing order to the web. Tech. rep.Stanford InfoLab, 1999.doi: 10.1016/j.comnet.2012.10.007. arXiv: 1111.6189v1.

[10]https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper

[11]Delegated Proof-of-Stake Consensus
https://bitshares.org/technology/delegated-proof-of-stake-consensus/

[12]http://news.8btc.com/the-impossible-triangle-of-blockchain

[13]https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ

[14]https://www.coindesk.com/2018-year-blockchain-ai-iot-converge/

[15]https://www.computerweekly.com/news/252433944/How-blockchain-can-secure-the-IoT

[16]https://github.com/bitcoin-core/secp256k1

[17]https://bitcoin.stackexchange.com/questions/21907/what-does-the-curve-used-in-bitcoin-secp256k1-look-like

[18]https://aip.scitation.org/doi/pdf/10.1063/1.4982580

[19]https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

[20]https://medium.com/hybrid-smart-contracts/hybrid-smart-contracts-ff963db9c702