# 亦来云白皮书

## 区块链驱动的智能万维网

亦来云基金会

2017.12.17

## >> 内容说明

此文档是亦来云白皮书 0.2 版本，在 0.1 版的基础上，我们重点增加阐述了亦来云战略目标和技术路线图等。未来我们会持续升级此文档，以体现亦来云最新发展状态。

关于亦来云白皮书的最新版本、路线图、团队、基金会治理、投资人、战略合作伙伴等信息，请随时访问亦来云官方网站。

## >> 联系我们

亦来云（上海）：

上海市虹口区塘沽路 463 号华虹国际大厦 11 层

邮编：200080

亦来云（北京）：

北京市海淀区成府路 45 号中关村智造大街 G 座 Plug & Play

邮编：100084

邮箱：

白皮书工作组：whitepaper@elastos.org

全球社区：global-community@elastos.org

亦来云资本：elastos-fund@elastos.org

公共关系：pr@elastos.org

投资者关系：ir@elastos.org

亦来云理事会：elastos-council@elastos.org

其他联系：contact@elastos.org

亦来云官网： http://www.elastos.org

亦来云基金会在新加坡注册。

## >> 版权声明

此文档著作权归亦来云基金会所有，保留所有权利。

## >> 免责声明

科技发展日新月异，为了更好推动亦来云项目发展，我们未来会不断完善现有技术方案及组织架构，但保持亦来云社区共治原则及亦来云代币分配方案不变。

# 目 录

# 1 项目背景

亦来云（Elastos）是全球第一个让区块链的可信能够传递到用户日常场景的操作系统。以区块链为可信基础，结合 Elastos 的沙箱隔离机制和网络隔离机制，让数字资产可以被确权、数量有限（稀缺）、可交易和可消费。让人人都能拥有数字资产，变现未来财富。从而将互联网打造为智能经济生态圈。

亦来云（Elastos）是开源的软件系统，其研发过程中受到了富士康等产业巨头超过两个亿人民币的赞助支持，已开源了上千万行源代码，包括超过四百万行原创开发的源代码。亦来云项目在陈榕的带领下，几百人团队开发多年，苦于一直没遇到合适的市场窗口期（像当年微软的 DOS 和 WINDOWS），直到遇上了区块链以及韩锋等业界代表人物。

Elastos 可以很好地保护数字内容、隐私不被泄露、不被窃取；而区块链可以为数字内容颁发 ID（权证），确认数字内容产权和可交易。两者结合为信息时代的互联网提供“私有产权”的经济基础。只有在产权明晰的基础之上才能产生经济、发展生产力。

陈榕和韩锋等人经过数十次讨论，对一个去中心化的全自动智能经济需要一个安全并且可用的操作系统达成共识。亦来云实现了“信任和计算分离”，使得大型去中心化应用（DApp）兼具“可用性”和“可信度”。解决了以太坊为代表的、智能合约虚拟机功能高度耦合的现有区块链系统的局限性。保证去中心化的应用完全跑在一个高性能的、可信安全的“财富互联网”上。

亦来云致力于在传统互联网上打造全新智能经济特区，亦来币是该经济特区内流通的基础代币。 亦来云创造者们期望把互联网智能经济推进到一个全新的高度。

## 2 技术背景

比特币实现了记录的可信性，以太坊实现了基于可信记录的可信计算。这就好像之前区块链只是纯文本 txt 记录内容，现在升级成了 excel 可以针对记录的内容做一些“宏”来完成自动计算。比如销售员帮助老板卖商品，交易成功以后自动分配一部分提成到销售员的账户。再比如：企业商品众筹，如果达到指定金额则转给企业开始生产；否则自动退还给参与者。

有了智能合约以后，我们不必再担心违约，不必再担心对方的诚信度。因为它像区块链账本一样会铁面无私地执行。从而让人们对可信社会有了更高的期待和期望。那么我们是否可以用它来做更多的事情？让我们生活的方方面面都能通过“可信”和“契约”来保证，省去很多互相不信任带来的成本？是不是可以用它来实现一个电子书商城？是否可以实现一个电影视频交易平台？是否能用它来实现游戏平台交易游戏？很遗憾，在以太坊的白皮书里明确说明了智能合约只适合于金融类项目、半金融类项目和在线投票等类型项目。我们通过分析发现以太坊为代表的智能合约存在以下问题：

>> 受限于区块链本身的存储能力，只能以很慢的速度保存有限的数据。一个参考数字是 2KB/14 秒。

>> 受限于区块链的存储能力和 EVM 运行机制，智能合约必须同步在各个节点中运行，这样才能对计算结果进行互相印证。CryptoKitties 的火爆导致以太坊堵塞的事件已经证明，单靠一条主链想运行所有智能合约是很难的。无论它有多少节点，都等价于一个节点的性能，这导致它负载有限。

>> 跟区块链记录只能写不能改的特性类似，智能合约一旦发布只能执行不能停止或修改。从逻辑上这是对的。对于约定好的“合约”、规则不能停止和改变，这样才能保护签约双方 / 各方的利益。但当出现 BUG 的时候，这也会让我们束手无策，比如 The DAO 攻击事件。而且数学上已经证明，我们不能证明写出的程序代码是否有 BUG。

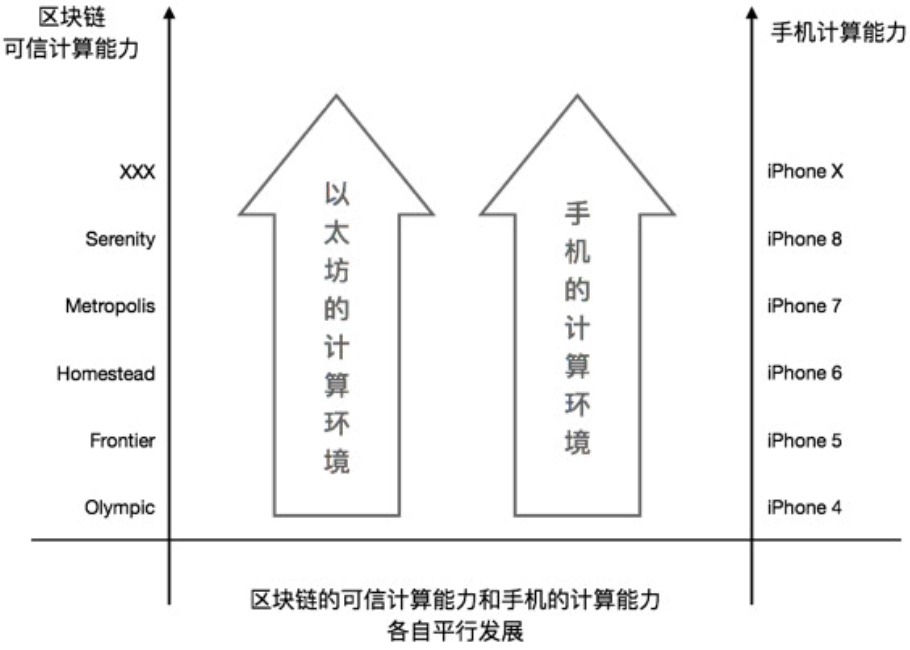
>> 智能合约本身，相关的数据记录，合约的执行都是在区块链上。而每个区块能打包的内容是非常有限的，几千台节点在重复做。这些数据和智能合约必须负担几千台节点的费用。是不是所有的程序都付得起这个费用？这就好像个人家庭的财务审计通常不会找四大会计所，价值太低。

>> 历史垃圾数据不停累计。一个智能合约一经发布就永远保存在区块链上。垃圾数据、冗余数据会给区块链的吞吐效率带来很多负面影响。以太坊已经发生过若干次区块拥堵事件就是很好的例子。

>> 执行智能合约的 EVM 的实现与区块链紧密耦合，无法独立分开。任何区块链的技术升级都可能影响 EVM，反过来也同样。

>> DApp 运行于用户的 OS 环境。如果数字内容（比如电子书）在 DApp 里播放，很可能会泄露内容从而破坏产权。

由于上述问题，用户无法在以太坊智能合约上实现看电子书、玩游戏、加密聊天等等。一方面性能体验无法接受；另一方面价格也可能贵的惊人。在现实生活中，用户已经习惯于在手机上运行游戏、看电子书、租借共享单车。如何能让区块链的可信和用户的使用场景连接起来，是我们希望解决的问题。




从上图看到，无论用户手里的手机多么强大，也帮不上以太坊分担计算；无论以太坊升级多少次也无法为用户手机的计算环境提供信用保障。因为是两条完全平行的发展路径永远不可能正交。

写段智能合约来发个 ICO 这或许真的很适合以太坊，但如果你想用它实现播放带版权的高清电影，恐怕是很难。各种形态的计算机芯片已经遍布我们的生活，有的在控制空调，有的在控制电灯，有的在手机里，最为熟知的在电脑里，他们都可以说是“图灵等价”计算机，但彼此换位使用却未必“等价”，试想我们把微信运行在冰箱的芯片里会怎样？我们不能因此说冰箱的芯片没价值，而恰恰相反，它很有价值——低功耗、廉价、稳定——只是它被用错了地方。基于区块链的 EVM 和智能合约也是如此，它的性能、编程模型、存储模型都决定了它不适合传统意义上的软件，更适合做数字资产转移、自动分账等偏金融方面的应用。对于除此以外的其它应用，亦来云基提出了一个新的解决方案：将区块链的可信和用户手机的计算能力结合起来，让各个层次和职能彼此泾渭分明正交。

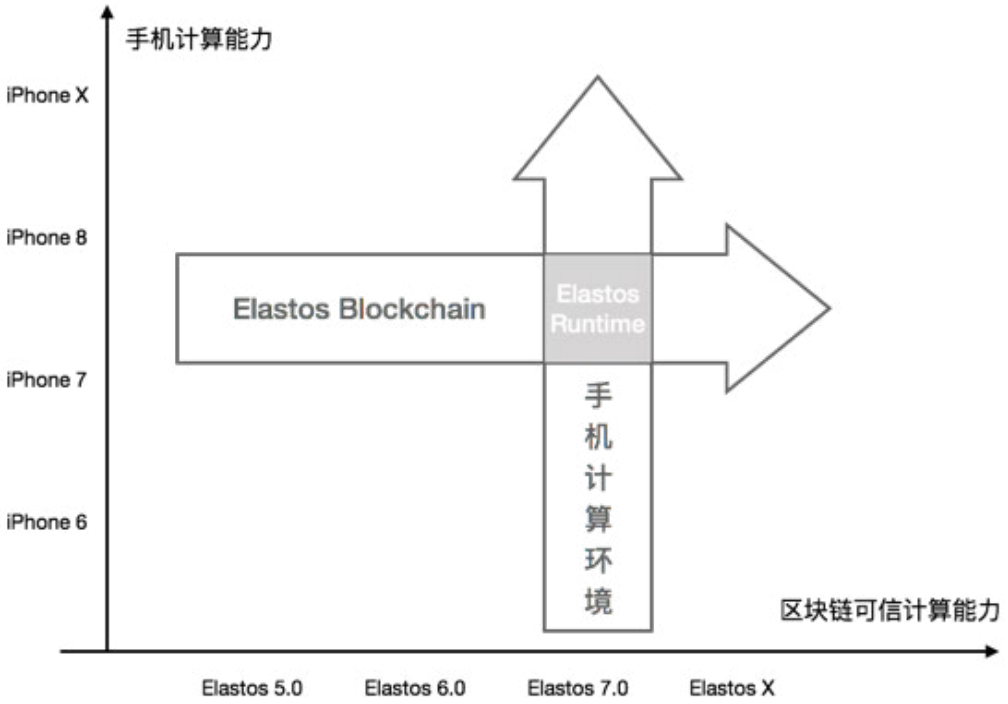
从连接用户日常场景的角度来说，以太坊 EVM 存在两个主要问题：

1. 单主链结构，计算能力有上限，无法扩容；
2. 区块链作为存储和计算空间，无法支持用户日常生活场景，无法应用数字内容。

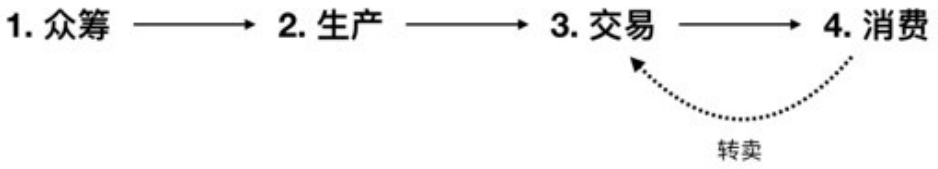
对于第一个问题，我们采用主链 + 侧链的弹性区块链设计结构。主链只负责基本的交易和转账支付；侧链执行智能合约支持各种应用和服务，每条区块链都是一台服务器。现实软件方案里，当服务器性能无法突破上限时，通常的做法不是去研发超级服务器，而是增加更多的服务器分流负载。在区块链项目上也同样，我们通过弹性侧链的方式让不同应用、服务共享一条侧链或分别部署在不同侧链，从而满足多样的需求。

对于第二个问题，我们通过 Elastos Runtime 将 App 运行在相互隔离的进程、通信受限的沙箱环境中。所有网络数据必须通过安全、可信、可识别身份的通道发送，这些身份识别和鉴权都来自于区块链身份 ID。这样就让区块链的可信传递到 Elastos Runtime。而 Elastos Runtime 可以有多种形态：可以是独立 OS，可以是 VM 虚拟机，可以是结合原生 App 的 SDK。

通过这样的设计方式，让以手机为代表的用户使用场景与区块链的可信空间产生了交集（正交），让 app 运行环境兼具二者的优点，让我们有希望彻底解决以太坊上智能合约功能不正交的问题。




通过这样的设计，让数字资产可应用、可消费、可使用。从而让数字资产完成了从生产、销售、消费的闭环流程。



## 3 亦来云：区块链驱动的智能万维网

亦来云的设计思想源于前微软资深软件工程师陈榕，他于 2000 年开始致力于开发世界第一个互联网操作系统，提出了“上网不计算，计算不上网”的基本设计思想，后经富士康等投资近两个亿发展成一个上千万行源代码的开源操作系统（github.com/elastos）,2017 年开始和区块链相结合，提出了智能万维网（Smartweb）的概念。

亦来云智能万维网（Smartweb）可以解析为四个层次：

>> 区块链及智能合约。区块链作为操作系统的信任区实现 “可信”。亦来云主链通过与比特币联合挖矿共享算力，依托比特币的 POW 机制保证可信度。同时亦来云还通过侧链提供服务和扩展第三方应用，以集群服务的方式提升区块链层面的计算能力，避免主链负载过重。亦来云支持在侧链上运行智能合约实现“可信计算”，可以灵活扩展区块链能力，但会严格限制合约的使用范围，仅用于针对数据资产的可信计算。

>> Elastos Carrier。Elastos Carrier 是一个完全去中心化的 P2P 网络服务平台，是亦来云支撑去中心化应用开发和运行的重要基础设施。

>> Elastos Runtime。Elastos Runtime 运行于客户的设备之上，实现“可靠运行时环境”。开发者通过开发 Elastos DApp 来实现使用（播放）数字资产的功能。VM 保证数字资产运行于区块链控制范围内，为用户提供消费 / 投资数字内容的能力。

>> Elastos SDK。传统意义的 APP，可以通过包含亦来云的 SDK 来扩展能力，获得身份鉴权、可信记录等区块链典型能力。

亦来云具有如下特点：

>> 恢复区块链本身的价值定位：可信数据库（可信账本）。只有最有价值的内容才保存在区块链，既经济，又高效。

>> 限定智能合约的能力不能滥用，它的定位类似于数据库的存储过程，用于区块链数据的自动计算和处理。

>> 基于区块链的可信记录和可信计算，我们可以为数字内容颁发权证（token）。通过权证确认数字内容的所有权。通过转移权证来交易所有权。让区块链成为数字内容的“产权中心”。

>> Elastos Runtime 运行于客户的 OS 设备上，费用、能力和性能都不受限，可以使用传统编程模型和编程语言开发 Elastos DApp，甚至可以直接移植现有软件。同时，通过沙箱与 OS 原生环境相互隔离，保证数字内容不会外漏。再通过 P2P 网络连接区块链服务，使权证在用户 OS 上仍然有效，继续保护数字内容。这样既可以低成本对接现有 App 生态，包括用户和开发者；又可以扩展和延伸区块链对数字内容的保护范围；还能让用户在手机上消费数字内容。

>> 对于更多的现有 App 来说，最轻量的方式是嵌入 Elastos SDK，通过它来访问部分区块链功能，从而实现部分去中心能力。比如可以通过 SDK 提供的身份 ID 来绑定自己的用户，进行身份鉴权；还可以通过 SDK 提供的 API 将重要内容的哈希散列保存在区块链，从而起到公证 / 存证的作用。通过这种方式可以最轻量级的对接现有应用生态，也让各种应用更方便的拥有区块链所带来的便利能力。

>> 通过 Elastos Runtime 将“区块链的可信记录”与“智能合约的可信计算”正交，我们让区块链上的数字资产可以从生产、交易、消费完成闭环。根据现代经济学理论和量子财富观，只有明晰、受保护的产权和合规的交易才能形成资本市场，才能成为未来时的财富。只有如此才能将现在的互联网发展成为“价值互联网”，直至“财富互联网”。

可以这样对比比特币、以太坊和亦来云：

比特币 = 可信记账
以太坊 = 可信记账 + 可信计算
亦来云 = 可信记账 + 可信计算 + 可信应用环境

有了 Elastos Runtime 保护的可信应用环境，数字内容才能真正产生价值，变现未来，被用户“消费”和投资。就好像给用户一张火星上的土地产权证，

在目前科技水平，这张证书基本没用。虽然它也可以去交易、可以去投资，但最终无法使用它的本体。如果宇宙空间科技提供一种能力把人类瞬间传送到火星，那么这张产权证就真的有用了。Elastos 就是这样一个桥梁，可以让用户在体验、效率、功效方面真正可消费数字内容，完成整个数字产品资本市场的闭环。

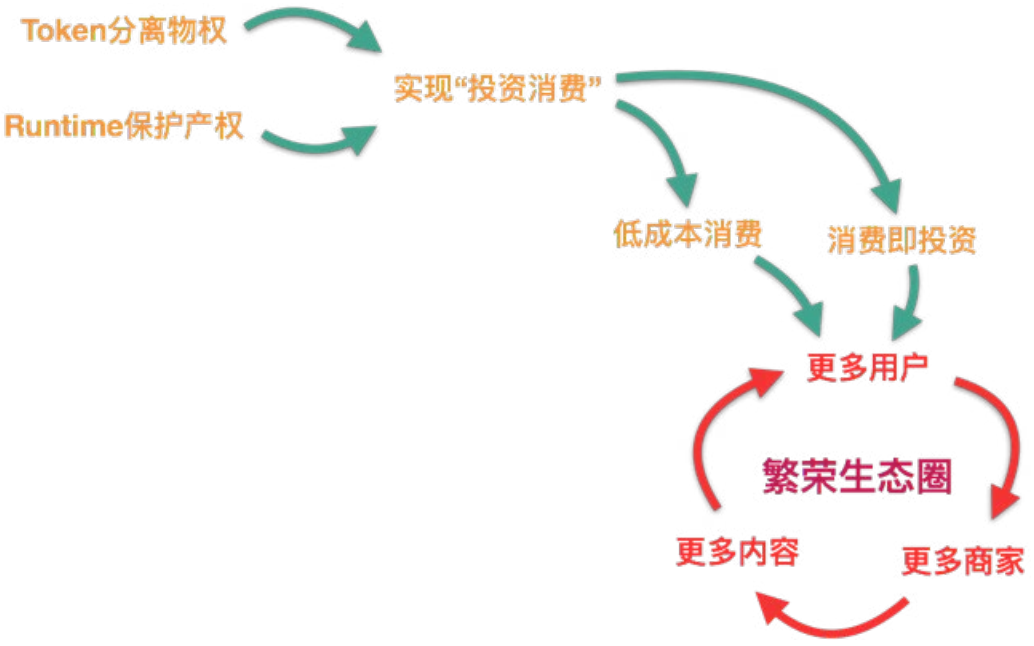
亦来云商业模式的基础：

1. 数字内容可以被使用无数次而仍然完好如初；
2. 可以在区块链上用权证标识确权；
3. 权证在区块链上可转移、交易，变成可变现未来的资本；
4. 凭借权证，可以在 Elastos Runtime 内消费 / 使用数字内容；
5. 可以为数字内容设置有限数量，制造稀缺，成为变现未来的资本。

基于上述基础，我们可以实现一种全新的用户投资消费模式：

1. 用户购买限量版游戏 App；
2. 在用户手机上的 Elastos Runtime 内玩游戏；
3. 不想再玩以后可以将这个游戏卖掉。因为这个游戏是限量版，并随着这个游戏口碑的传播，让它在二手市场里乘风破浪涨了好多。帮助用户既享受了数字内容又赚取了“早起”的收益，变现了未来时的财富。

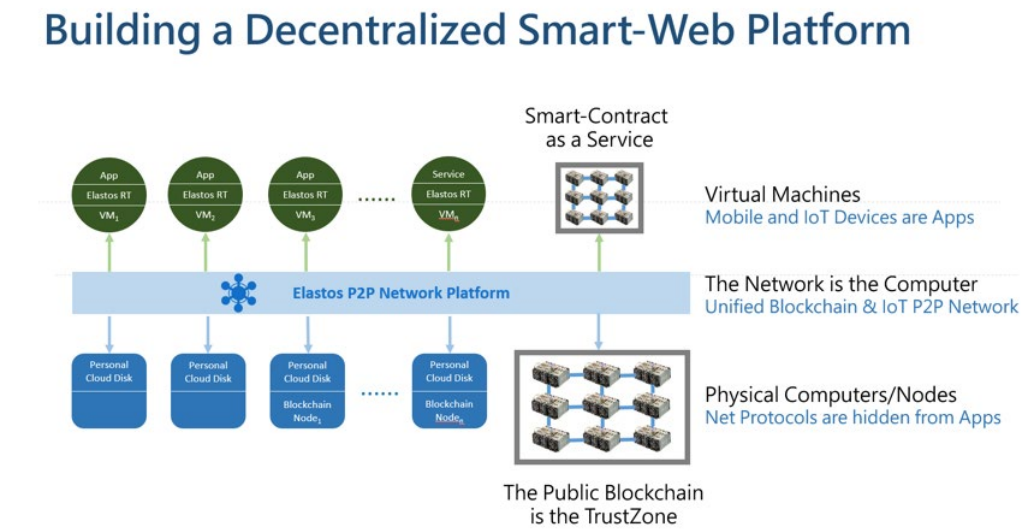
我们称这种既投资、又消费的行为叫“投资消费者”( 蚂蚁金服首席战略官陈龙回复，韩锋的文章时提出的概念 )。通过帮助用户取得这样的效果和价值，可以吸引更多用户加入、使用 Elastos Runtime。当聚集大量用户以后，会有更多的数字内容生产者（开发商）加入我们的平台生产内容、发布内容。更多的内容带来更多的用户；更多的用户促发更多的内容。从而形成正向循环，最终产生数量巨大的、有价值的数字内容和财富。




而亦来币是整个平台运转的自然等价物。需要用亦来币支付手续费、购买基础服务和购买数字内容，变现未来时财富。全部亦来币可以看做是平台所承载的全部数字内容和用户对其未来的“标价”。随着内容的增加和用户的增多，亦来云的同步 GDP 增长，源源不断地有更多数字资产变现未来，这为总数近似恒定的亦来币带来了升值基础。

我们希望通过亦来云，让互联网可信、让数字内容成为资产、让创作者获得财富、让消费者同时也成为投资者，让信息互联网变成财富互联网。

# 4 架构




## 4.1 信用体系

自从上世纪七十年代，美元与黄金脱钩，布雷顿森林全球信用体系崩溃，全球信用生产完全依赖人的信用。如今比特币挖矿产业正在逐步演变为未来全球信用生产的基础设施及战略性资源，这标志着人类社会信用体系与自然资源脱钩的态势正在发生微妙的改变，预示着人类信用资源又开始向自然资源（算力）回归的大趋势。

亦来云联合创始人韩锋于 2016 年 3 月发布《生产全球信用的人们》报告，第一次指出中国已经占到全球比特币挖矿产业算力 50% 以上。同时，亦来云联合比特大陆、BTC.TOP 、BTCC、币信等战略合作伙伴成立“区块链挖矿信用生产联盟”，致力于推动将比特币算力升级为信用生产的公共服务，进而抑制能源消耗和碳排放的问题。

亦来云区块链携手其战略合作伙伴进行比特币联合挖矿，这意味亦来云区块链发布第一天即获得极其强大的算力保障。我们致力于成为世界级的公有链，为全球区块链创新，特别是亦来云生态提供信用生产的基础服务。

## 4.2 数字资产确权、交易和流通

在“比特世界”里，数字资源几乎无成本复制与传播。但由于数字资源无法确权，虽然被海量生产、流通、消费，而且创造价值，但是无法创造财富。从而导致盗版、山寨横行，原创动力不足等副作用，数字不能有效变成财富使虚拟数字经济发展遇到了瓶颈。区块链技术已经证明数字货币是可行的，在新的智能经济模式中，传统“原子世界”看不见的思想、人脉、数据、纠缠等会成为财富的主体，这即是量子财富观。

亦来云为数字资产的确权、交易和流通提供基础设施。将数字资源通过区块链发布到网络上时，将被确权，数字资源将成为区块链上被信任的数字资产，可以用于流通和交易。发布数字资产必须有亦来云钱包，钱包帐户余额须足以支付矿工费，然后发起确权交易请求，请求包括所有者钱包地址、资源 URI、数量、单价等信息，然后计算资源的哈希值，把该交易作为 UTXO 记录在链上。当资产确权交易记录被发布到区块链以后，该资源成为可以用于交易的数字资产，购买交易生效后，客户购买的数字资产的归属权也转移到客户账户名下，除了使用价值外，也可以再次出售。

## 4.3 去中心化应用（DApp）

基于当前的数字货币和区块链技术，至今还没有可以跟主流应用媲美的去中心化应用。这是因为逻辑上的区块链世界计算机虽然是图灵等价的，但其计算能力、IOPS 等关键指标都比较弱，区块链已经不堪重负。

亦来云区块链设计采用了主链、侧链模式，所有的智能合约、应用都运行在侧链上。用户通过亦来云操作系统，可以很方便地开发出安全的去中心化应用。在不使用亦来云操作系统的情况下，通过 ElastosRuntime，可以开发出同样效果的基于 Android、iOS、PC、Mac 等的去中心化应用。同时我们建立亦来云应用商店，分发去中心化应用。

# 5 亦来云区块链

如同手机操作系统需要一个信任区（Trust Zone）保存关键数据，比如用户指纹，亦来云区块链相当于亦来云生态的信任区，为整个生态提供信用、交易基础服务。

面对智能经济和去中心化应用需求，亦来云区块链采用主链、侧链设计方案，即每个应用都可以独立开设一个侧链。亦来云区块链提供内置的、完善的、易用的侧链支持，侧链有多种共识算法模块供用户选择，侧链可以发行代币，主链和侧链可进行双向资产转移。所有侧链与主链共享算力，因此所有侧链都具有和主链一样的安全性。同时整体系统能耗可以实现最小化，避免分头挖矿带来巨大能源消耗和碳排放的问题。

## 5.1 交易和区块设计

亦来云区块链结构参考了现有的经典的数字货币系统设计，包括区块验证必要的前一区块头哈希、交易默克尔树根哈希、用于工作量证明算法的计数器（Nonce）、时间戳、难度目标等内容，这样一个链式的存储结构，能够让交易获得所有累积在上面的工作量证明的保护，并且实现去中心共识的目标，进而成为全自动的信用生产体系。

同时我们也吸取了现有的数字货币、区块链系统的经验教训，整体上采用主链、侧链相结合的设计思路。将验证脚本从交易结构中拿出去，减少了交易空间占用，避免了延展性攻击。侧链是亦来云众多 DApp 运行的基础，因此亦来云主链结构要提供对侧链的支持，要能够方便资产在主链和侧链间转移。

## 5.2 联合挖矿

亦来云区块链采用比特币联合挖矿机制，比特币作为主链（Parent Blockchain），亦来币作为辅链（Auxiliary Blockchain），矿池通过部署联合挖矿代码，矿工同时向比特币和亦来云提交工作量证明，无需耗费额外算力即可享有双重奖励，增加了矿工在采矿竞争中的收益。

通过联合挖矿机制，亦来云区块链拥有极其强大的算力保障。为全球区块链创新，特别是亦来云生态提供信用生产的基础服务。

除了充分利用既有比特币计算资源并且更为环保之外，联合挖矿技术还具备之前并未被人们充分认识的潜在价值：

>> 可以多层次信任传递。亦来云主链依托于比特币主链联合挖矿，采用 POW 共识的亦来云侧链也可以依托于亦来云主链联合挖矿，依次递推，这种信任关系可以在很深的层次传递，这有利于分层次结构化组织区块链生态。

>> 依托于联合挖矿的辅链并不需要多个节点的共识。极端情况，一条链只需要一个节点就可以了，而且这并不影响链上帐本信息的可信度，这种优势是其它任意一种区块链共识算法都不具备的。这非常有利于使用分叉机制复用侧链的实现代码，扩充侧链的计算能力。

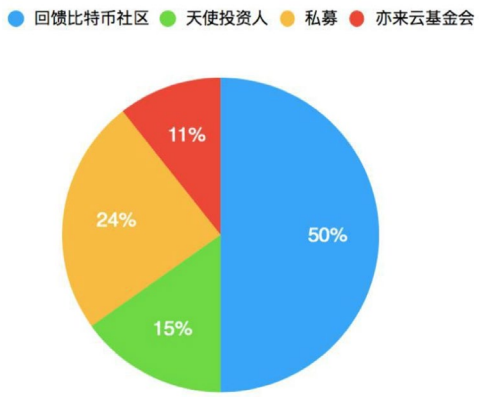
## 5.3 代币分配方案

亦来云代币（ELA Coin），简称亦来币（ELA），是亦来云区块链上的原生代币，用于交易、支持数字资产、支付区块链交易手续费等。

我们使用 ELA 作为亦来云代币的基本单位，中文名称：亦来币或者艾拉。此外，向数字货币启蒙者 Satoshi Nakamoto 致敬，我们用 SatoshiELA 作为亦来币最小货币单位，并缩写为 Sela，中文名字是：赛拉。其换算关系如下：

1 ELA = 10^8 Sela

为了促进亦来云生态运转，并参照美元总发行量（约 2000 万亿美元），以及比特币总发行量（2100 万亿聪），在亦来云区块链创世区块中一次性创设：3300 万亿赛拉，即 3300 万个亦来币。



亦来币的分配方案和实施细则如下：

| 亦来币<br>（单位：万） | 用途 | 说明 |
| --- | --- | --- |
| 1650 | 生态建设 | 以亦来云区块链创世区块诞生的时间点为基准，确定比特币持有者，向其免费发放亦来币，具体规则如下：<br>>> 目的：回馈数字货币社区，创造有效流动性；<br>>> 数量：比特币持有者获得相等数量的亦来币；<br>>> 渠道：只通过授权数字货币交易所发放亦来币；<br>>> 方式：亦来云基金会将通过授权交易所一次发放，即，不会自动获得亦来币；<br>>> 所有最终未被申领的亦来币将统一注入亦来云资本，用于投资亦来云生态建设，即，不会被用于亦来云基金会的日常运营。 |
| 500 | 天使投资人 | 亦来云团队及其相关资源提供方组成了亦来云项目天使投资人，未募集的剩余额度归入亦来云基金会。 |
| 800 | 众筹<br>（私募及公募） | 投资人社区是亦来云的中坚力量，将长期支持和推动亦来云的发展。募集所得数字货币全部归亦来云基金会所有，用于开发亦来云生态平台及前期试运营。未募集的剩余额度归入亦来云基金会。 |
| 350 | 亦来<br>云基金会 | 亦来云基金会预留：<br>>> 支持亦来云基金会运营；<br>>> 通过亦来云资本投资亦来云生态项目，打造亦来云生态圈。 |

为了弥补类似用户钱包丢失等自然损耗的流通量，以及保持其支撑的智能经济生态微量通胀等，亦来币每年保持固定同比 4% 的增发。增发的亦来币将在比特币联合挖矿中伴随每 2 分钟左右的区块生成同步产生。为了保持亦来云生态的可持续发展，自亦来云区块链正式上线后两年内，此部分亦来币将在亦来云基金会和矿工之间按比例分配，亦来云基金会拥有 30%，矿工拥有 70%。

## 5.4 侧链

如前所述，以区块链技术构建的任意一条链的计算能力都是小于等于一台计算机的，这显然无法适应互联网层面的多种应用需求，这也是直到今天区块链技术依然无法大规模应用于互联网的根本原因。亦来云团队深刻认识到了这点，所以自亦来云项目起步之初就提出了“区块链的发展应放弃主链思维”的指导思想。

基于这一指导原则，亦来云主链只为上层架构提供可信的亦来币交易服务，同时限制智能合约的执行，因此主链上的服务功能是纯粹并且有限的，我们希望在主链层面更多的关注区块链服务架构的可扩展性而不是某种功能或者性能。

亦来云通过主链对侧链更好的支持来扩展区块链层面的基础服务能力，这种层次化和结构化的设计思想能从根本上解决目前区块链技术的计算能力问题，就如同从单机计算时代发展到分布式计算时代。这是亦来云在链层面的结构性创新，我们认为其重要性要远远高于某种局部技术或者共识算法的创新。

除了支持第三方能够比较方便的在亦来云公链上构建侧链外，亦来云本身还会架构一些提供基础服务的侧链，比如 ID 服务、Token 发行服务、快速支付服务以及数字资产交易服务等等，我们称之为亦来云区块链集群服务，它们都是亦来云基础设施的重要组成部分。

在主链和侧链的接口中，交易转账是其最核心的部分。从主链向侧链转账，意味着要把主链资产转变为侧链资产，转账目标地址是对应侧链在主链上的联合签名地址，转账过程需要保证转账交易能够自动被侧链识别并为转账人在侧链对应账号充值对应价值的侧链代币。

通过随机秘密以及对应的哈希，我们可以构造必须提供秘密才能解锁的交易脚本。下面是转账过程的示意步骤：

1. 转账用户 A 生成一个随机秘密，以及对应的哈希；
2. 用户 A 在主链上构造给侧链在主链上的联合签名地址转账的交易，交易的解锁条件除了需要提供联合签名地址的私钥签名，还要提供用户生成的秘密；
3. 用户 A 将上面的交易以及秘密对应的哈希发送给侧链转账处理节点；
4. 侧链转账处理节点在侧链上生成给用户 A 在侧链上的发币交易，这个发币交易的锁定脚本要求用户 A 提供秘密哈希对应的秘密本体以及用户 A 在侧链上的私钥签名；
5. 用户 A 提供秘密，从侧链上获得代币；
6. 侧链在主链上对应的联合签名地址根据上面提供的秘密，从主链获得代币。

侧链向主链的转账过程相当于从主链的联合签名地址中转账亦來币到用户在主链的帐户。下面是转账过程的示意步骤：

1. 转账用户 A 生成一个随机秘密，以及对应的哈希；
2. 用户 A 在测链上构造提币交易，交易的解锁条件是提供用户 A 生成的秘密；
3. 用户 A 将上面的交易以及秘密对应的哈希发送给侧链转账处理节点；
4. 侧链转账处理节点在主链上生成给用户 A 在主链上的发币交易，这个发币交易的锁定脚本要求用户 A 提供秘密哈希对应的秘密本体以及用户 A 在主链上的私钥签名；
5. 用户提供秘密，从主链上获得代币；
6. 侧链在主链上对应的联合签名地址根据上面提供的秘密，解锁用户 A 的提币交易，销毁对应的代币 。

为了控制联合签名地址上亦來币的安全性，这个“联合签名地址”会限制只能发起上面描述的“提款转账”交易。

### 5.5 智能合约

在主链上提供强大的智能合约会导致每个节点要获得整个网络的最新状态，就要把未运行的智能合约都运行一遍，而只有打包交易的矿工运行合约才能得到交易费，所以对于单纯验证的节点来说是在浪费计算资源，如果合约调用次数频繁或者数量庞大，都会对执行合约带来巨大压力甚至无法实现。

为了避免这样的问题，亦来云主链只有限地支持用于数字代币交易的智能合约。侧链可以支持智能合约，而且各个侧链可以独立设计其智能合约功能，比如支持 NEO 区块链的 NeoContract。

## 6 Elastos Carrier：去中心化 P2P 网络

ElastosCarrier 为亦来云生态提供去中心化互联网基础服务。其节点可以运行在任何网络环境中，包括家庭或者办公环境的局域网内部，采用基于 UDP 的透明 NAT 穿越技术，及相关辅助设施，可以实现任意节点都可以被连接，同时也可以实现任意两个节点间的直接连接。这样可以让任意节点的能力都可以被充分利用，从整体上提升网络的效能。

基础服务包括去中心化域名服务、去中心化计算服务、去中心化存储服务。为开发去中心化应用程序（DApp）提供了基础性的支持。在这样的环境里，用户可以拥有自己的数据，拥有自己的计算，充分保护了用户隐私。同时，也可以随时把自己的设备通过亦来云区块链租借给他人，根据计算量、存储量获得对应的亦来币激励。

# 7 Elastos OS：安全的通用操作系统

Elastos OS 是以安全为核心目标的，面向 IoT 设备、树莓派等创客设备、移动设备等的通用操作系统。提供原生的、完整的亦来云生态编程环境支持。最新的第三版从 2013 年 5 月开始产品化迭代周期，已达到 Beta 版水平，测试运行于 Moto X（XT1085）手机、Lamobo-R1S 智能路由器之上，全部源代码规模超过千万行。

安全方面，ElastosOS 禁止应用直接创建进程，不允许应用直接访问 TCP/IP，由系统自动创建和查找部署于本地、周边、云里的微服务，自动生成远程调用及事件回调，规避从第三方应用或服务发起网络攻击的可能性，并隔离病毒传播。

Elastos OS 提供了原生的、完善的去中心化应用开发支持，可以方便访问 ElastosCarrier 网络，获取所需基础服务，方便访问 ElastosChain，获取信用和交易服务。开发出来的 DApp 可以方便使用亦来币进行交易，同时也可以方便处理其他数字资产，比如：程序代码、数据、电子书、音视频、游戏道具等，包括确权、交易、流通。

系统采用 C/C++、JAVA、HTML5/JS 三类语言并重的开发模式，其 C++ 编程 API 基本对应安卓 Java API，实现云、管、端三位一体统一管理。JavaScript、Java 还是 C/C++ 语言写的应用程序模块相互调用，无需手工编写 JNI，真正做到“一次编程、到处运行”。支持 CAR 构件技术，下面是一个使用 CAR 构件技术编写的 C++ 代码和 JavaScrip 代码交互的示例：

```
var eventHandler = (function() {
        return {
            OnEvent:function(i) {
                var s = 'OnEvent, i: ' +
                        JSON.stringify(i);
                elastos.log(s);
            },
        }
})();

var module = elastos.require('Demo.eco');
var obj = module.createObject('CDemo');
obj.addEventHandler(eventHandler);
obj.doTask();
```

JavaScript

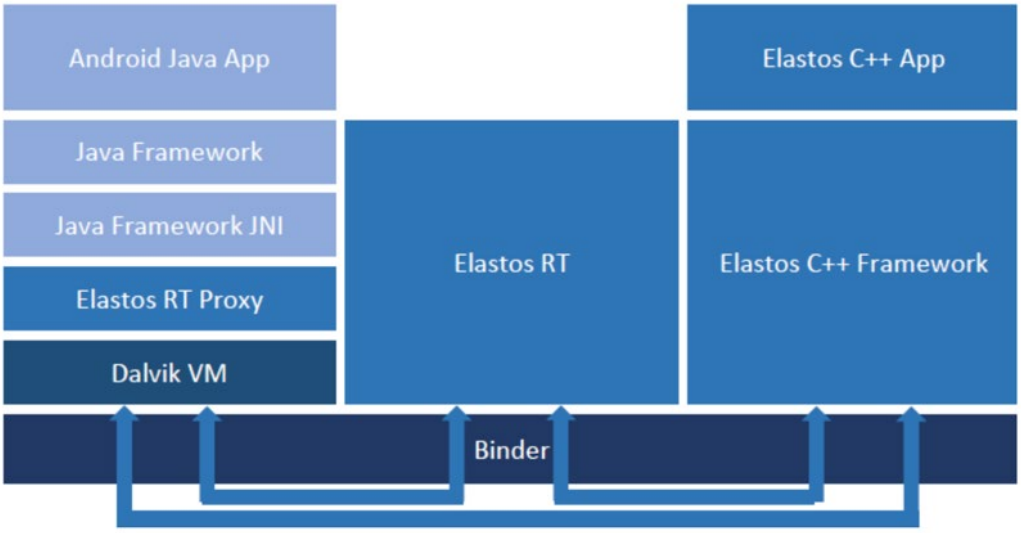
```
Module
{
    interface IEventListener {
        OnEvent(
            [in] Int32 id);
    }

    interface IDemo {
        AddEventHandler(
            [in] IEventListener* listener);

        DoTask();
    }

    class CDemo {
        interface IDemo;
    }
}
```

Demo.car (compiled to .cls)

```
...

ECode CDemo::AddEventHandler(
    /* [in] */ IEventListener* listener)
{
    m_Listener = listener;
    return NOERROR;
}

ECode CDemo::DoTask()
{
    m_Listener->OnEvent(9);
    return NOERROR;
}

...
```

CDemo.cpp (compiled to .eco)

Elastos OS 的 C++ Framework 采用类安卓的应用接口，方便应用的开发和迁移。在 Elastos OS 上，甚至可以直接支持运行 Android 应用，其实现模型如下：




可以认为 Elastos Runtime 就是 C++ 版的 Java 虚拟机和 Java 框架，也可以称为 CVM。Elastos OS 服务和应用在 CVM 中运行，让同样的服务更容易适配不同的硬件和节点。

# 8 Elastos Runtime：运行时环境

虽然通过 ElastosOS 可以立刻获得原生的、完善的去中心化应用编程环境支持，但在很多时候，用户会继续使用现有的操作系统。这时可以采用 ElastosRuntime，即亦来云去中心化应用运行时环境，同样提供了完善的支持。我们将提供 Elastos Runtime for Android，Elastos Runtimefor iOS，Elastos Runtime for GNU/Linux，开发者可以根据自己需要灵活选择。下面我们将通过一些示例代码来展示亦来云去中心化应用编程风格。

## 8.1 P2P 网络接口

DApp 之间可以直接通过构件接口互相访问、调用，无需（也无法）编写网络操作代码，编程体验更加简单、直观、安全可控：

```

TrustID myfriend = "0xE94b04a0FeD112f3664e45adb2B8915693dD5FF3";
IChat * pChat = CChat::New(myfriend);
pChat->Chat("hello");

```

上面网络代码不再需要考虑如何封包、拆包、加密、解密，不再设计“协议”，都由 ElastosRuntime 的 CAR 接口完成，只需要编辑下面的接口 CAR 文件：

```

interface IChat {
    Chat(String message);
}

class CChat {
    interface IChat;
}

```

然后再编写对应的接口函数即可完成相应功能：

```

ECode CChat::Chat(String message) {

    // your code ....

    return NOERROR;
}

```

相比传统的基于 Socket API，基于 Elastos Runtime 编写 P2P 网络应用更加安全并且非常简单。

## 8.2 数字资产接口示例

如前面例子所展示的，我们在网络通信时不再依赖 IP 地址或者域名，目前的互联网并不可信，但基于 Elastos Runtime 开发时，我们给予亦来云的可信区，即亦来云区块链，Elastos Runtime 会进行相应的验证和确认。

```
33
34  ECode _CChat::Chat(String message) {
35
36      ... ...
37
38      // 检查TrustID是否存在
39      if (Exist(trustID) == FALSE) {
40          return ERROR;
41      }
42      // 检查当前APP ID是否在黑名单
43      if (InBlackList(_Current_App_TrustID) == TRUE) {
44          return ERROR;
45      }
46      // 检查当前用户ID是否在黑名单
47      if (InBlackList(_Current_User_TrustID) == TRUE) {
48          return ERROR;
49      }
50      // 检查当前调用次数是否超过上限
51      if (Called_Count > MAX_CALL_COUNT) {
52          return ERROR;
53      }
54
55      // 更多检查和校验
56      ... ...
57
58      ec = CChat::Chat(message);
59
60      ... ...
61
62      return ec;
63  }
64
```

进而可以进行数字资产的交易，下面是检查所有权演示代码：

```
66
67  TrustID aMovie = "0x32B77CBB265175D1A927c9A3F816de577BDDdE05";
68  TrustID owner = "0xd4fa1460F537bb9085d22C7bcCB5DD450Ef28e3a";
69
70
71  if (Elastos.RT.Trust.CheckOwner(owner, aMovie) == TRUE) {
72      // yes, He is its owner.
73  }
74  else {
75      // error
76  }
77
```

下面是交易演示代码：

```
82
83  Elastos.RT.Trust.SendTransaction(buyerID, sellerID, 1000, aMovieID);
84
```

# 9 亦来云基金会

亦来云项目历史悠久，其前身可以追述到公元 2000 年陈榕归国创业，从那时起到现在，陈榕致力于开发一个安全的、通用的、能适应网络时代的操作系统。2017 年，亦来云项目转型为由社区驱动的、全球性的自由开源软件项目，其开发的软件源代码和文档等都以自由开源软件许可证发布。

我们通过亦来云基金会来运营和推动亦来云项目，打造亦来云生态。我们积极拥抱自由开源社区、数字货币社区，互相交流学习，共同促进人类文明的进步。亦来云基金会已经在新加坡注册成功。

## 9.1 全球性社区

全球亦来云爱好者、开发者、文档维护者、社区活动组织者、亦来币持有者等等组成了亦来云全球性社区，这是亦来云项目的根基，也是亦来云生态蓬勃发展的土壤。打造亦来云全球社区是我们最重要的工作之一。

在全球各地，亦来云本地社区以亦来云用户组（Elastos User Group）的形式存在，每个用户组都有负责人、运营团队，以及在亦来云官网上对应的介绍主页，他们都是亦来云的支持者，以自愿者的方式投入社区工作。用户组负责组织、维护和发展本地亦来云社区。主要工作包括：推广数字货币、区块链理念，研讨亦来云技术，参与亦来云项目开发，文档撰写和翻译，组织本地社区月度聚会，协助组织亦来云官方全球性活动。

## 9.2 人才培养

现在还是数字货币、区块链的早期阶段，行业高速发展，人才缺口极大。亦来云创始成员 2016 年 9 月通过 DACA 协会在清华大学 iCenter 启动“我们都是中本聪”计划，以培养高水平的区块链技术人才。该计划实施以来，

为业界培养了大量人才，不少其中优秀人才加入了亦来云团队，逐渐成为亦来云区块链团队的中坚力量。亦来云基金会将持续支持 DACA 协会公益培训项目，和清华大学 iCenter 合作，使其发展成区块链领域的黄埔军校，不断为中国区块链社区培养技术开发力量。

### 9.3 生态建设

亦来云是智能经济的技术基础设施，为开发去中心化应用提供了强有力的技术支持，最终将发展成亦来云生态。全球性的亦来云社区和持续的人才培养是实现亦来云生态的重要基础。与此同时，为了加速建设亦来云生态，我们将在亦来云基金会下设立亦来云资本（Elastos Fund），用于专项投资开发基于亦来云生态的去中心化应用。

亦来云生态让“比特世界”更安全、更智能、更富有，打造一个全新的“财富互联网”！