

CryptoXBox: A Box can protect your secret use Cryptography and Decentralized BlockChain Platform

by CryptoXBox Team
@2019-03-27

为什么选择区块链和加密技术

在互联网上使用公钥加密技术已经能很方便的加密传输敏感信息，结合区块链技术可以完成资产的安全、隐私地转移。

CryptoXBox 将会使用公钥加密技术，保证只有私钥的持有者才能打开盒子，同时盒子的状态上链，保证只有你自己打开过盒子。

CryptoXBox 使用场景

每一个人都有很多想要隐藏起来的東西，每栋楼都有很多的房间和门，每个门上面都有锁；邮寄的食品总是担心快递员吃掉，点了外卖担心被外卖员往饭菜里吐口水。人与人之间从来没有真正的信任，如果能创造一个只有两个人或者只有自己能打开的空间，我们内心的焦虑就会少很多，现在 CryptoBox 可以解决大家的烦恼。

点对点的通信

公钥加密技术是目前最安全的加密技术，可以用著名的情书问题来解释公钥加密的原理：

- 1、小明生成了一个包含公钥和私钥的密钥对。私钥由小明自己保管。
- 2、小明写了一封情书，约好晚上 7 点在老地方见面，想让韩梅梅传给李雷，但是担心韩梅梅的八卦
- 3、于是小明把自己的公钥交给韩梅梅，让她取回李雷的公钥
- 4、小明利用李雷的公钥加密了情书，再由韩梅梅传递给李雷
- 5、李雷收到韩梅梅传递的情书并用自己的私钥解密，然后回了一封信，表示会赴约，并用小明的公钥加密，然后由韩梅梅传回。
- 6、但是，当天晚上小明和李雷都没有等到对方。
- 7、原来韩梅梅替换了他们的公钥，并且解密替换了信息，最后韩梅梅分别赴约，度过了快乐的一夜。

在现实世界中模拟点对点通信

在上面的例子中小明和李雷的失败就在于韩梅梅拦截并替换了他们的公钥，此时双方都拿到韩梅梅的私钥且并不知情，此时即使小明和李雷都使用了加密和签名也无济于事。所幸真实的情况并没有这么糟糕，往往我们还能安全的交换公钥。

CryptoXBox 的灵感

信任问题可能是当今最严重的问题，我多次看到很多团队在研究利用区块链进行产品溯源，结合我对区块链的理解，对区块链是否真的能对产品进行溯源和实际效果深表怀疑。

再一次接触产品溯源后我决定从另一个方面解决信任问题，CryptoXBox 就是这样一个容器，可以 100%原封不动的把商品从生产厂家或者商家传递到消费者手中，不管运输途中经历了什么，能接触商品的只有商家和消费者。因此，商品是否合格是否假冒就只和商品的生产厂家有关。

后来我发现，CryptoXBox 的用途远不止如此。

与产品溯源的区别以及优势

产品溯源：如果能证明商品或生产材料的源头，这就是优质产品，应该多卖钱

CryptoXBox: 如果某个产品有问题，那么这个销售商或者生产厂家一定有问题
不难看出 CryptoXBox 真正解决了信任问题。

Token 发行以及流通

为了更好的让 CryptoXBox 服务大众，我们将会设计一条公链，用于 CryptoXBox 和人类之间进行交互。CXB 作为燃料用于执行智能合约，同时也用于对运行节点的回报。

100 0000 0000 CXB 会被初始发行，在挖矿和燃烧 CXB 执行合约的双重调节下会处于一个平衡状态。

由于 CryptoXBox Team 从未接受过任何私募，因此计划出售 30 0000 0000 亿 CXB 用来换取资金用于 CroptoXChain 的开发和 CryptoXBox 的设计。

CryptoXBox 生态建设

CryptoXBox Team 会设计安全有效的 CryptoXBox 标准并且开发 CryptoXChain,协助对 CryptoXBox 有兴趣的企业接入 CryptoXChain 或者定制自己的设备，为用户正确使用 CryptoXBox 做咨询和教学。

CryptoXBox Foundation

负责 CXB 的售卖，CryptoXBox Team 的经费，已经建立 CryptoXBox Alliance

CryptoXBox Alliance

当 CryptoXChain 和 CryptoXBox 开发接近完成时，成立产业联盟，负责生产与推广

CryptoXBox Project TimeLine

2019-03-27 这一天，CryptoXBox 正式诞生了

2019-04-01 ~ 2019-04-30 预计花一个月时间完成 CXB 的初始售卖，并成立实体公司

2019-05 ~ 2019-12-31 前完成公链的初始版本开发

2020 年 6 月前推出首个 CryptoXBox 硬件，成立产业联盟

计划永远赶不上变化，根据不同的财务状况，项目实现的进度快慢是不能预测的，甚至有失败的可能。CryptoXBox Team 并没有能力对不可测的未来负责。