

CYBEX

CYBEX: 去中心化数字资产交易所

**白皮书 (beta)
version 1.0**

作者 CYBEX 团队

www.CYBEX.io

t.me/joinchat/Gmz68UScWa3dbskAG2hUug

medium.com/@CYBEXexchange

ABSTRACT 摘要

CYBEX 是一个去中心化交易所，旨在打造比现如今中心化市场更透明、更安全、流动性更强的数字资产交易平台。CYBEX 是由全球志同道合的合作伙伴在去中心化网络中共同建立和运营的一个生态系统。其核心是基于 Graphene 区块链引擎，该引擎高效安全，能够通过权益证明机制，以每秒 10 万次交易的速度进行扩展。交易所还包括其他特色，如原子交换功能，能够推动跨链交易；网关的硬件多重签名托管功能，可确保加密资产管理的安全性；内置 ICO 发行平台和模板，来实现去中心化 ICO；价格稳定货币以尽量减少交易波动风险；还有一支在业务发展和运营方面记录完备的核心团队，确保交易所不会有门可罗雀之时。

TABLE OF CONTENTS 目录

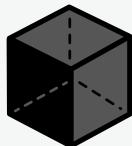
1.	中心化面临的问题	3
2.	去中心化交易所	4
2.1	CYB 代币	5
2.2	见证人节点	5
2.3	委员会	5
2.4	权益证明机制	5
2.5	投票	6
2.6	预算	6
3.	主要功能	7
3.1	原子交易	7
3.1.1	为什么是原子交易?	7
3.1.2	CYBEX 中的原子交易	8
3.1.3	操作细节	9
3.1.4	促进流动性	10
3.2	加密资产托管网关	10
3.2.1	网关	10
3.2.2	热钱包	11
3.2.3	冷钱包	11
3.3	去中心化公售平台	13
3.4	价格稳定货币	14
3.4.1	加密资产的波动性	14
3.4.2	比特币作为抵押品	15
3.4.3	利润激励	15
3.5	移动端用户界面	16
3.6	业务拓展	17
3.7	主流业务代币化	18
4.	开发工作路线图	19
5.	CYBEX 团队	20
5.1	核心团队	20
5.2	顾问团队	21
6.	风险提示	22

1. THE CENTRALIZATION PROBLEM

中心化面临的问题

随着市场对数字货币以及底层区块链技术兴趣的增加，其估值与种类也呈指数级增长。截止撰稿时，根据 CoinDesk 报道，ICO 融资额累计已增至约 38 亿美元，涉及 200 多个项目，而这个数据可能只是整个市场的冰山一角。

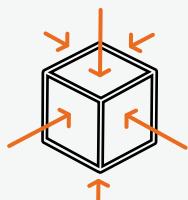
如今，大部分数字货币在中心化平台交易，但这类平台正面临着以下挑战：



- **不透明**: 大多数中心化的交易所都存在数据严重不透明的情况，交易所往往可以利用信息的不对称来操纵价格，甚至是挪用客户资金进行交易，而这造成的后果往往会导致交易所运营出现重大问题，从而给投资者带来不小的损失。



- **流通性差**: 大多数项目发起的 ICO 处于未完成或未启动状态，项目代币尚未真正分发给投资人，而是在承诺好发币日期后先进行 IOU 交易（“欠条”交易）。这类 IOU 交易流动性通常有限，即使能够交易也只是在发布 ICO 的平台上先交易，或者就是支付昂贵的上线费用到其他中心化交易所上线。



- **安全性低**: 中心化交易所容易受到 DDoS 攻击，这不仅会严重干扰交易，还会损害投资者对这一过程甚至整个 ICO 模式的信心。而且，中心化交易所也是诸多黑客的下手对象，例如 Mt. Gox, Bitstamp, Bitfinex, DAO, CoinDash 等等。

在 2017 年 9 月中国政府发布相关政策禁止 ICO 之前，CYBEX 团队曾创建了中国最大的 ICO 平台——ICOAGE。在 6 个月的运营期间，ICOAGE 成功帮助近 40 个项目（如 TenX, Status, iEx.ec, EOS, Qtum, Storj 等）募集价值逾 1.7 亿美元的数字货币。

ICOAGE 作为中心化 ICO 平台，曾遭受无数次 DDoS 攻击，平均每次攻击量高达 120gb，不过凭借其完备的安全措施，平台用户并未受到损失。也正是这类高密度、高强度的攻击，促使团队开始搭建去中心化平台，以防止此类攻击。

2. CYBEX: A DECENTRALIZED EXCHANGE

去中心化交易所

CYBEX 是真正的去中心化数字资产交易所，基于著名的区块链解决方案 BitShares 及其底层石墨烯区块链库升级扩展而来，而目前 BitShares 应用生态已经壮大。



在 EOS 作为 BitShares 的延续上线后，CYBEX 会将底层技术转移到 EOS 上。

CYBEX 致力于提供更安全、高效、易用的交易体验，为了实现这一点，团队专注于协议及应用层的创新，结合商业专业知识以确保交易所健康运行。关于主要功能详细介绍请参考本文第三部分。

下面是关于 CYBEX 生态系统核心概念的简单介绍。

2.1 CYB代币

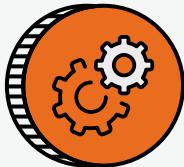
CYBEX 网络的基础代币是 CYB，可以分割为 10 万个子单位。CYB 具有一定价值，能够在区块链上进行转移，并且通过曲线 secp256k1 的椭圆曲线数字签名算法(ECDSA)保障其安全性。与大多数数字货币不同，CYB 本身不是一种货币，它还包含以下核心使用功能：



- **参与权:**CYB是CYBEX生态系统的燃料，该代币所赋予的所有核心权利与特权都是权益证明，在其生态系统中享有参与、投票以及贡献的权利。



- **交易所媒介:**CYB是CYBEX生态系统中的基础交换媒介，生态系统中的所有费用均已CYB来计价。



- **功能:**CYB可用于交易所内所有金融工具，例如价格稳定资产等。

2.2 见证人节点

见证人节点会收集交易，捆绑到一个区块，然后广播到网络中。他们的角色和比特币生态系统中的矿工类似，只不过 CYBEX 的共识算法采用的是权益证明机制，而比特币采用的是工作证明机制。见证人节点每成功捆绑一个区块，就可以从有限的储备池获得一笔费用。而储备池的容量及费用金额由生态参与者投票决定。

2.3 委员会

经过挑选所成立的委员会负责管理生态系统内部工作。在CYBEX上线后，所有生态系统的运营，包括分工、产品、费用、预算等均由委员会决定。

2.4 权益证明机制

和比特币的工作量证明机制(POW)相比，权益证明机制(DPOS)不会像 POW 那样为了避免高成本、低效率而消除信任的需要。

生态系统中的每位用户都可以给任意数量的节点投票肯定。当任意节点获得超过所有票数的 1% 时（占生态系统总量的比例）就有资格成为见证人节点来生成区块并获得相应的报酬。每个维护周期（一天）会在票数统计好后更新一次见证人节点名单。

每个见证人节点轮流生成区块，每轮见证人节点生成一个区块的顺序或排期是确定好的，交易平均在一秒内确认。所有见证人节点轮完后，会打乱顺序开始新一轮。如果某个见证人节点在其时间段内没有生成区块，那么系统会跳过这段时间，由下一个见证人节点生成下一个区块。

见证人节点可以准备多种情境以备在不同机器、不同地点进行接管。这样可以缓解 DDoS 攻击量。如果所有见证人节点都没能生成区块，那么网络就会停止，用户也无法投票(交易)选出新的见证人节点。不过这种事件发生的概率很低，而且权益相关者也可以通过投票挑选更多见证人节点。

2.5 投票

用户可以针对 CYBEX 生态系统的每个运行环节投票，而不仅仅是挑选见证人节点。从费用机制到区块间隔再到交易大小，所有网络参数都能通过投票来调整。

用户甚至可以投票选择代表来替他们投票，也就是代理投票。这样可以确保生态系统中的每个人即使没有时间或倾向来衡量每个问题，他们也能选出合适的人代表他们完成。

2.6 预算

CYBEX 有一个预算池来支付完成各类任务的生态参与者（例如见证人节点）。CYBEX 在发行之际会留出一个预算池，所有后续预算分配、任务及相关费用结构都由后续投票决定。

CYBEX 内部所收取交易费用的 50% 会销毁，因此 CYB 的总供应量会逐渐减少，剩余代币的价值会逐渐提高。



3. KEY CAPABILITIES

主要功能

尽管 BitShares 在其概念及底层技术方面都拥有很高的创新性，但作为加密资产交易平台并未得到广泛采用。

我们认为，通过协议层的创新来促进便捷安全的交易，应用层的创新来改善用户体验，以及通过注入商业及运营专业知识，都能够大大提高去中心化交易所的采用率。

为此，CYBEX 带来了以下一系列改进与功能，

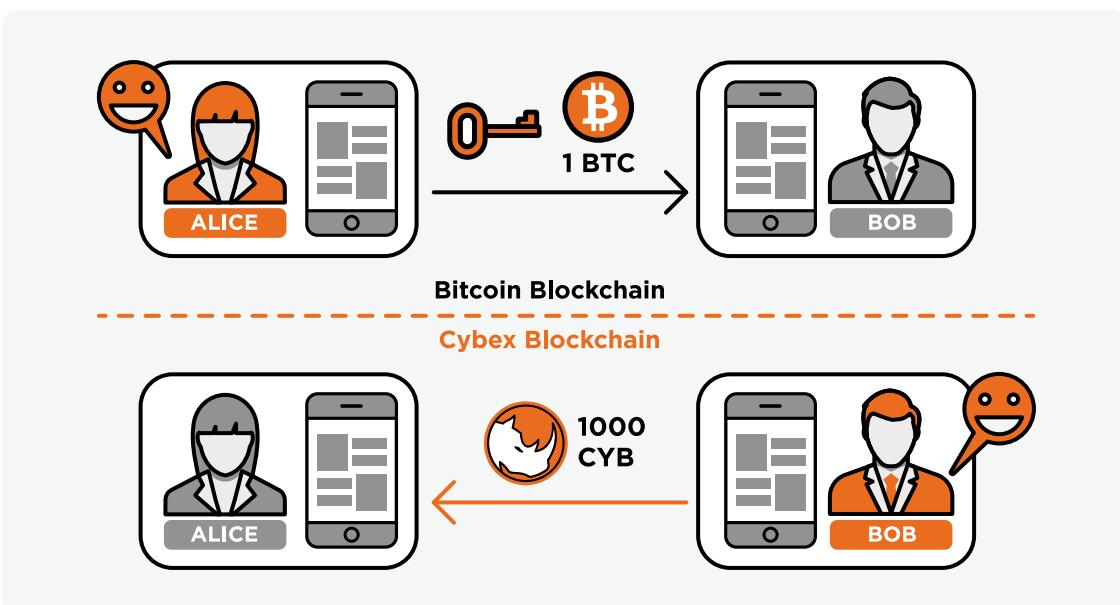
- 原子交易
- 加密资产托管网关
- 去中心化ICO平台
- 价格稳定货币
- 移动端用户界面
- 业务拓展
- 主流业务代币化

3.1 原子交易

经过挑选所成立的委员会负责管理生态系统内部工作。在 CYBEX 上线后，所有生态系统的运营，包括分工、产品、费用、预算等均由委员会决定。

3.1.1 为什么是原子交易？

原子交易，或原子跨链交易，就是在无需信任任何第三方的情况下，实现一种加密货币与另一种加密货币之间的交易。

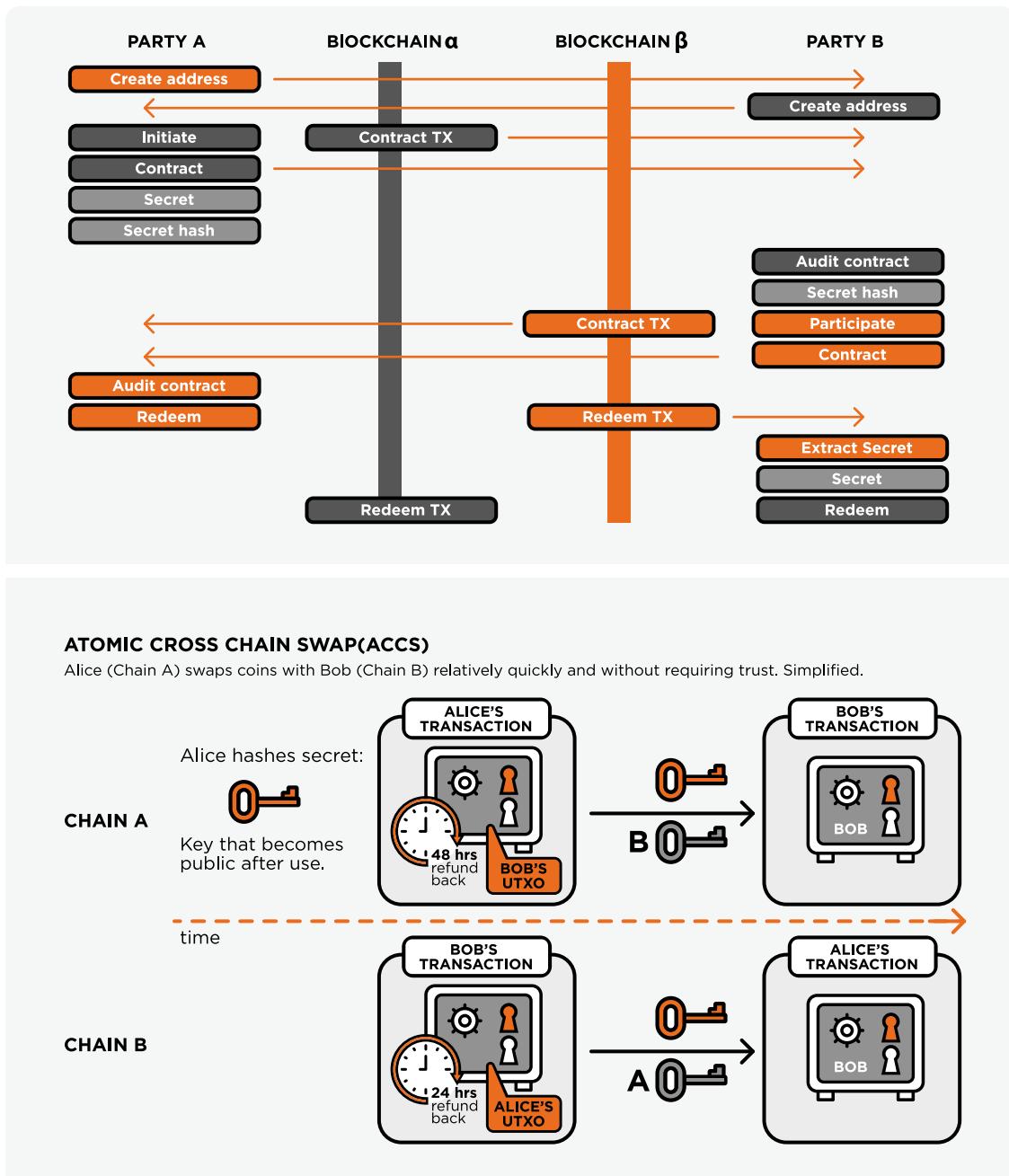


例如，Alice 将比特币打到 Bob 的比特币地址，反过来 Bob 要将 CYB 打到 Alice 的 CYB 地址。但是，由于两条区块链结构相异，且一旦挖矿，交易便无法撤销，因此这种交易过程不会消除交易任一方不信守交易承诺的违约风险。通常的解决方案就是引入一个彼此都信任的第三方（例如中心化交易所）提供托管服务，但如我们所见，信任这样一个中心化的实体也是很难实现的。原子跨链交易就在无需第三方介入的情况下解决了这一问题。

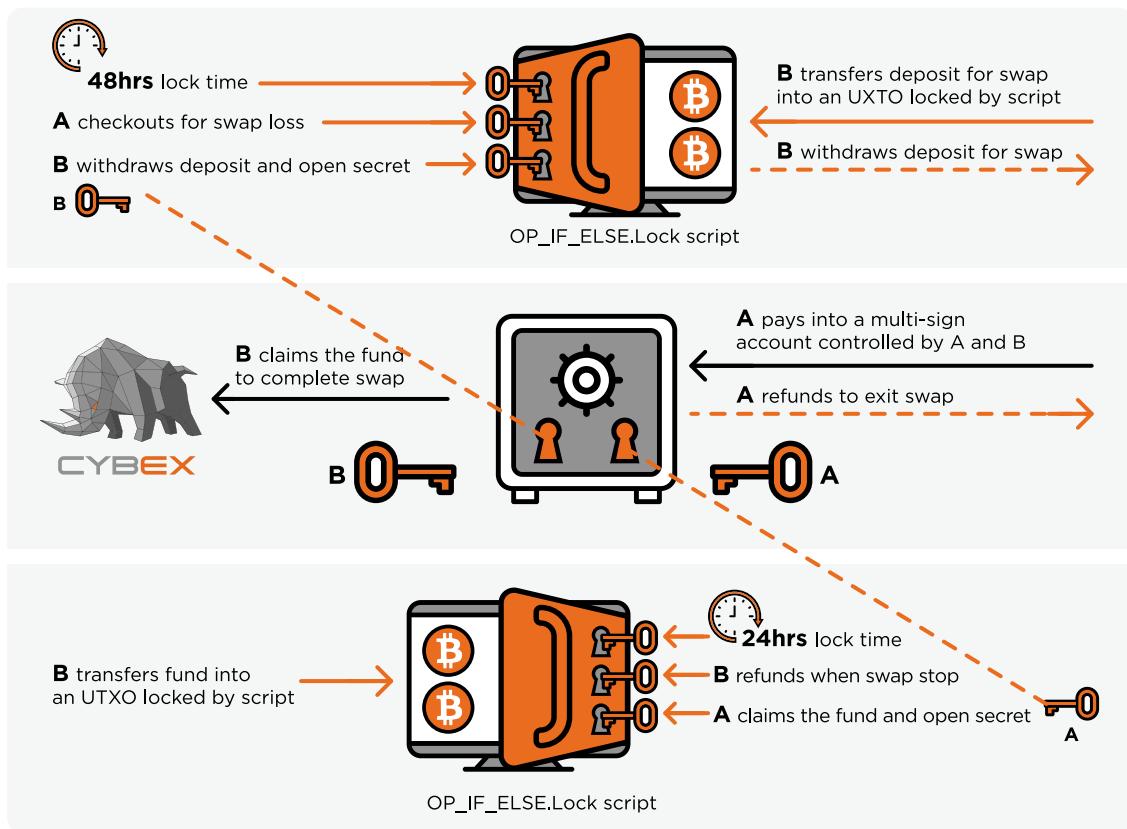
3.12 CYBEX中的原子交易

CYBEX 与比特币之间的原子交易需要每一方都将资金支付到锁定账户中。就 Cybex 而言，即多重签名账户；就比特币而言，即具备锁定脚本的 UTXO。莱特币创始人李启威(Charlie Lee)便使用莱特币与比特币、Vertcoin 以及 Decred 进行了交易，成功实施并证明了原子交易的可行性。但是这种交易方案仅在与比特币区块链有着类似脚本的区块链之间才能够发挥作用，而且，交易双方还都需要支持 CLTV(Check Lock Time Verify)功能。

使用 CLTV 脚本就可为退款操作设置锁定时间窗口，例如，发起人为参与者进行付款或者赎回资金设置了 48 小时的锁定时间，参与者则为发起人赎回资金设置了 24 小时的锁定时间。这种锁定时间的退款方案就保证了原子的完整性，当一方退出交易过程时，任何一方都可以完全撤回其资金。



由于 CYBEX 不具备类似于比特币的脚本系统,因此,我们使用了多重签名账户来锁定发起人向参与者支付的 CYB(假设发起人支付 CYB),并使用脚本来锁定 UTXO 中参与者支付给发起人的比特币。但多重签名方法的一个缺点就是无法实现复原与退款过程的。CYBEX 设定了保证金要求来激励并保障交易的完整性,从而解决了这一问题。



CYBEX与比特币之间的原子交易

3.13 操作细节

在CYBEX中,原子交易始于公钥与密钥哈希交易的切选机制(cut and choose)



通过一系列的交互,交易双方将获得对方的临时公钥以及拥有高概率证明的密钥哈希,这些都是由同一个私钥生成的。然后使用公钥以及私钥哈希在比特币脚本中验证资金赎回的真实性。这种机制就保证了不同加密货币(如比特币和 CYB)以一种完全点对点的方式直接进行安全交易。然而,交易对手方的匹配与流动性始终都是去中心化交易所面临的一大挑战。

3.14 促进流动性

原子交易只是解决了以无需信任的方式进行跨链交易的问题。然而却并未解决交易双方彼此匹配的问题。事实上，已经从技术上证明了许多原子交易都依赖于交易双方不仅了解彼此，还会通过某种即时通讯系统持续沟通的基础上。

为帮助促进流动性，CYBEX 会以交易对(比特币 vs CYB，CYB 作为一种代币将在众筹后上市不同中心化交易所)在外部交易所的价格向所有见证节点进行喂价。见证节点随后将在链上发布喂入价格。用户在链上以其预期价格提交交易订单，CYBEX 见证节点将自动匹配这些订单。

在生态系统的初始引导阶段，CYBEX 将激励有经验的做市商和交易机器人提供所需的流动性增强。CYBEX 核心团队或相关生态系统合作伙伴开发运营的一些传统网关将与原子交易功能长期并存，以提供高度安全的 IOU 服务。而且 CYBEX 已经推出了一个项目，将 CYBEX 客户端整合到支持定制比特币脚本和多重签名，以及第二阶段硬件安全级别的多加密货币钱包中。该项目能够推动在单一钱包中实现一键交易，从而更加便于用户使用。

CYBEX 及其他主流加密货币之间的交易能力将创造出许多金融工具，例如能够以全球普遍采用的货币(例如美元)维持平价的价格稳定加密资产，它对于便利且防审查的商业模式具有高度的实用性。通过超额抵押、免除交易对手方风险、智能合约担保的区块链贷款等方式来追踪传统标的资产(例如比特币)的价值，就可以实现这一点。

3.2 加密资产托管网关

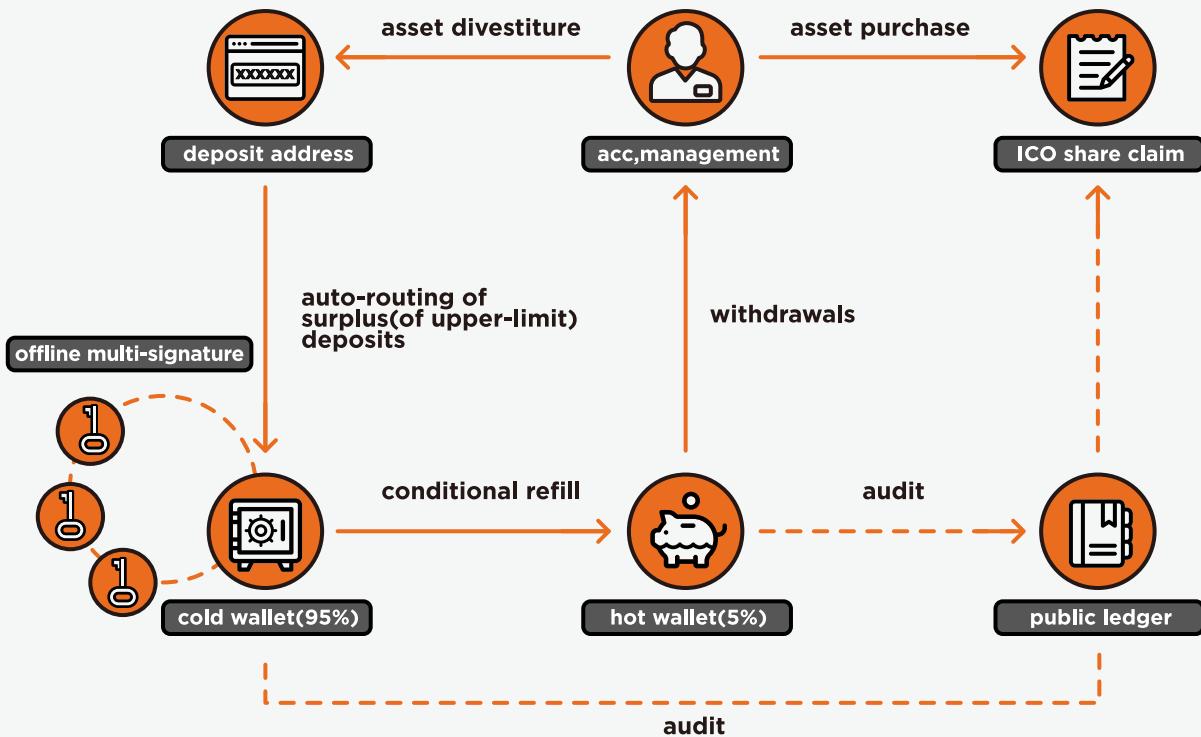
3.2.1 网关

推荐使用网关将资金转入或转出 CYBEX 网络。它们简化了将资金从一种基于区块链的加密货币转移到另一种加密货币的过程。

网关基本上等同于依赖交易所的偿付能力来兑现货币的标准交易模式。一般来讲，网关会发行以其标志为前缀的资产，如 CYB、APE、APD。这些资产完全由人们存入网关的真实比特币或以太币或任何其他货币所支持。

因此理论上，CYB.BTC 就等同于在 Poloniex 上获得的 BTC，而这里的 BTC 也可以 POLO.BTC 作为前缀。在这两种情况下，用户都是依靠服务提供商来保持偿付能力，从而支持他们发行资产的价值。

CYBEX 在其生态系统合作伙伴 Nebula Crypto-Assets 的支持下，拥有一个独立的加密资产托管服务网关原型，确保其持有加密资产的安全。这一极为重要的安全性功能将有助于简化网关设置，并降低对高价值加密资产进行中心化管理的风险。



3.2.2 热钱包

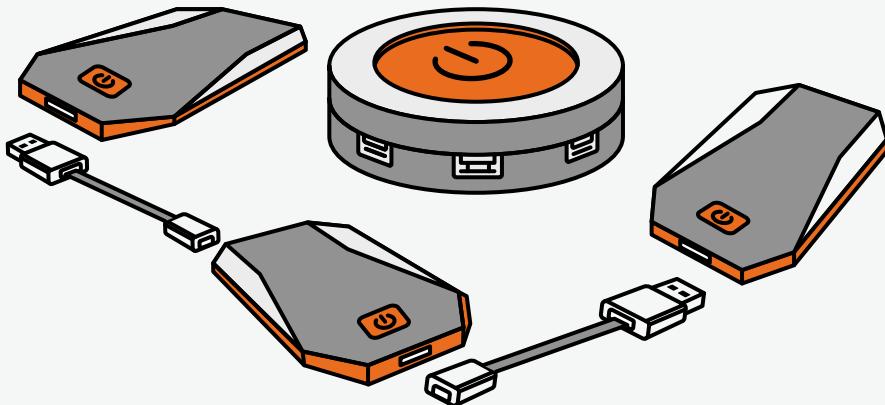
系统会将持有的一小部分资产（例如 5%）保存在在线热钱包中，而该热钱包内将包含用户将其加密资产存入 CYBEX 账户页面时生成的所有充币地址。用户可自发从网关提取资产，提取的资产将由热钱包自动发送。热钱包将随着时间的推移逐步发展，从而优化热钱包缓冲区的流入、流出以及大小，将冷钱包执行的对外交易数量降至最低，保证最大程度的安全性。

3.2.3 冷钱包

对于网关持有的剩余加密货币资产（例如95%），CYBEX建议使用由我们的生态系统合作伙伴 Nebula Crypto-Assets Custody设计的高安全性冷钱包解决方案。

Wallet of Crypto-Assets for Gateways

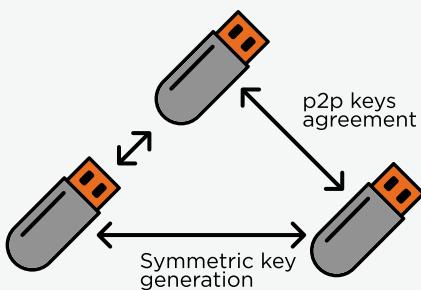
- Offline secret sharing hardware wallet
- What you see is what you sign



多重签名方案被认为是以加密的方式确保高价值资产安全的一种解决方案。比特币区块链从早期阶段就通过无状态脚本支持多重签名。以太坊社区开发了智能合约来实施这一方案，但一直以来智能合约的安全性都是令资产持有者感到担忧的一个问题，这种担忧在 2017 年发现一系列严重漏洞（例如 Parity 事件）之后尤为凸显。其他货币（例如门罗币）目前也尚未发布多重签名功能。

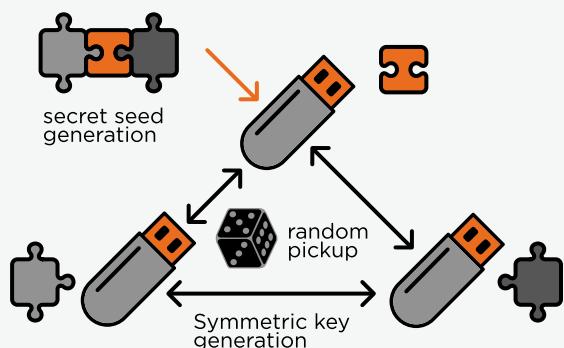
Nebula Crypto-Assets Custody 采用秘密共享算法为多个签名者设计了一个单一签名解决方案。为了解决在内存中复原完整私钥的安全性问题，该设计使用了银行级别的 wys/wys（所见即所签）硬件来实现仅在硬件密钥内部共享并复原秘密。

Decentralized Keys Agreement



- Secrets only exist in U-key COS
- Decentralized keys agreement generates communication key
- A random picked U-key for the secret seed generation
- Distribute secret shares into every U-key

- True random generator FIP140-2
- Security elements EAL 4+
- 128*64 OLED display
- Support ECDHE and BIP32
- SHA3, AES256, SHA256, Secp256k1



共同签名过程可以在线下或线上以去中心化的方式完成。整个签名过程的安全性纳入了点对点 ad-hoc 密钥白皮书算法，从而确保 P2P 通信的安全性，并不取决于 USB 集线器或互联网路由的安全性。

3.3 去中心化公售平台

CYBEX 不仅仅是交易资产的平台，同时也是一个通过公开发售(Crowd-sales)来首次发行资产并筹集资金的平台。为促进公开发售的发展，CYBEX 将提供一套可供发行人选择的合约模板。其中一个模板就是 Vitalik Buterin 以及 Jason Teutsch 提出的“交互式代币发行”。这一设计的目的就是为了解决传统公售所面临的难题：如何为代币估价？

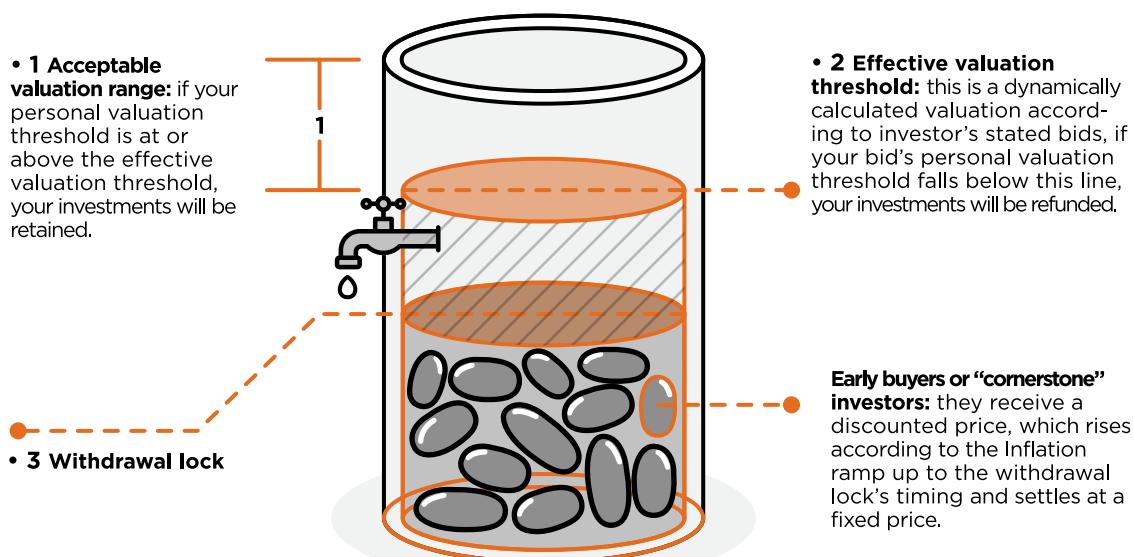
与潜在买家可以根据现有及潜在未来收入源来估计股票价值的股权分配活动不同，代币发售可能根本不会表现出任何预计收入。由于传统的分析无法估计出新代币的初始市场价值，买方就必须依靠一些新迹象或方法来决定这些代币的市场价值。另一方面，代币发行人也面临着不了解其买方的空前挑战。尤其是买方无法辨别两个不同的购买地址是否属于同一个人。

完美的代币公售模式应该解决双方面临的难题，

- 定额货币至少能认购到固定比例的代币
- 以及人人都能够参与

如果一个单位的货币至少能够认购占总代币量为 p 的代币，那么公售总收入就不能超过 $1/p$ 。

很明显，任何固定的估值方案都无法保证普遍参与，因此我们需要构建一个公售协议，确保如果每个参与者在每次估值时具体指定期望的认购数量，那么最终代币成本与百分比的比率满足所有买方(在估价和参与两方面都能够得到满足)。



拟议公售协议包括：

- **基本步骤：**在每个区块时段，买方既可认购代币，也可自发从公售中提取资金。买方指定他们愿意参加的最高销售估值，如果销售数量到达这一个人门槛，那么买方的出价就会被取消，同时买方会收到退款。我们增添了对销售下限触发的出价激活的支持。
- **提取锁定：**在经过一定数量的区块之后，系统将不再允许买方自发提取资金。例如，在为期 30 天的公售中，智能合约可能会允许买方在前 20 天自发提取资金，但在最后 10 天的时间里，智能合约将仅允许自动提取资金。
- **通胀轨迹：**早期认购代币的买方将获得一定的折扣价格。最高优惠可能为 20% (如今公售典型折扣率)。该优惠在提取锁定初期将平稳下降到 10%，直至公售末期降至为零。

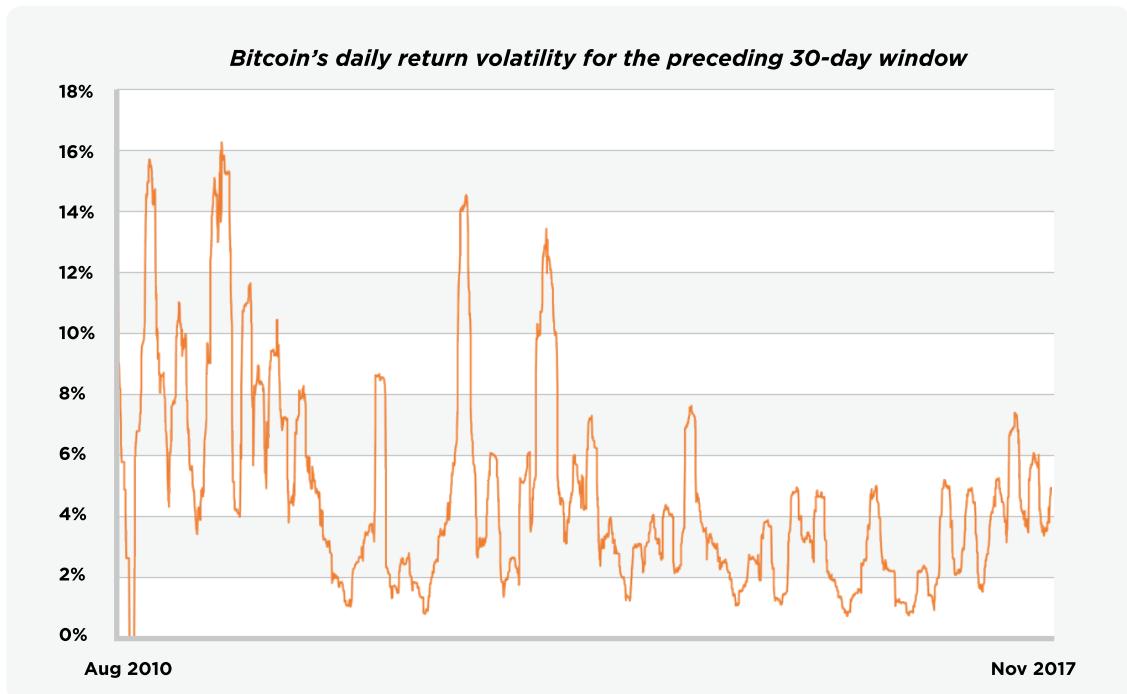
为了在 CYBEX 中实施公售合约，开发者会对一些对象进行修改，例如在本地数据结构的对象扩展中添加具备锁定属性以及交易操作字段的资产发行。并将重新设计 vesting_balance_object/db_balance 以及钱包 API、list_balances、claim_balances 等的逻辑。

3.4 价格稳定货币

3.4.1 加密资产的波动性

持有任何一种资产都会面临的主要困境之一就在于其无法预见的波动性。一种资产对另一种常规资产(如美元等法币)的价格波动越大，持有这种资产的风险也就越大。如果波动性高到了一定程度，这种资产的风险就会过大，以致于无法在日常商业活动中使用。

加密资产是一种相对较新的资产类别，其波动性通常比非数字资产更大。“比特币／美元”定价的波动性在逐渐降低，但仍保持在 5%-6%。相比之下，更传统的资产的波动性，比如“黄金／美元”定价或“美元／欧元”汇率，则只有 0.5% 左右。



减少这种波动性及风险的方法之一在于交易所要拥有价格稳定的资产，与不易波动的资产挂钩，比如美元。这种资产可以作为一种稳定的锚定物对其他加密资产进行估价，每个单位的这种资产都可以为人们带去可预测的回报。

我们打算让 CYBEX 持有价格稳定的资产，其中一种是一系列与比特币挂钩的稳定货币，与美元等稳定货币等价，我们将之称为“cyb.USD”。接下来我们要描述的是价格稳定资产可能的实现方式。

关于这种货币的想法并非首创——例如，BitShares 的生态系统中就存在这种货币的交易。但是，这个生态系统中的挂钩货币存在两种问题：

- 挂钩货币本身就波动性过大（从而背离了挂钩的目的），因为它由流动性相对较低的加密资产 BTS 担保
- 挂钩货币的发行量过小，因为缺少激励

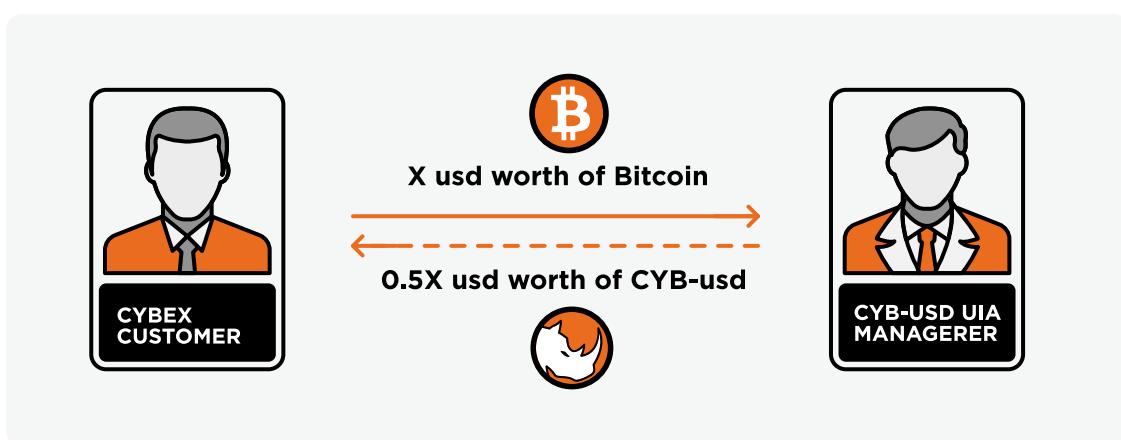
在 CYBEX 的设计中，挂钩货币的抵押品以比特币为基础，而比特币是一种更加主流且流动性更高的加密资产。我们设置的利率也会向比特币持有者提供发行 cyb.USD 的激励，从而避免 BitShares 生态系统中的问题。

3.4.2 比特币作为抵押品

价格稳定资产的理念在于当它被用来与其他资产进行交易时，交易比率是固定的。例如，我们希望确保每一个 cyb.USD 都能兑换 1 美元。

但是，由于法币在 CYBEX 等加密货币交易所中的使用仍存在法律和监管上的不明确性，我们的 cyb.USD 会被用来和更加稳定且更具流动性的加密货币进行交易，如比特币和以太坊。在本文中，我们就以比特币作为例子来阐释。因此，每个 cyb.USD 要能够兑换价值 1 美元的比特币。在撰写此文时，1 个比特币的交易价格约为 9080 美元，也就是说，我们希望 1 个 cyb.USD 能够兑换大约 0.00011 个比特币。

如果你希望能持续用 cyb.USD 兑换比特币，那么就需要确保有很多比特币可以用来交易。也就是说，任何发行(出售)cyb.USD 的人都需要拥有相应数量的比特币作为抵押品。还记得吗，我们刚才说过“比特币／美元”的价格颇不稳定，为了抵御这种不稳定性，我们要求 cyb.USD 的发行人留出更多的比特币(比如两倍的量)来覆盖每一个 cyb.USD。举个例子，发行 1 个 cyb.USD——可兑换 0.00011 个比特币(等同于 1 美元)，就需要留出两倍多的比特币，也就是 0.00022 个(相当于 2 美元)，来覆盖任何可能出现的波动。

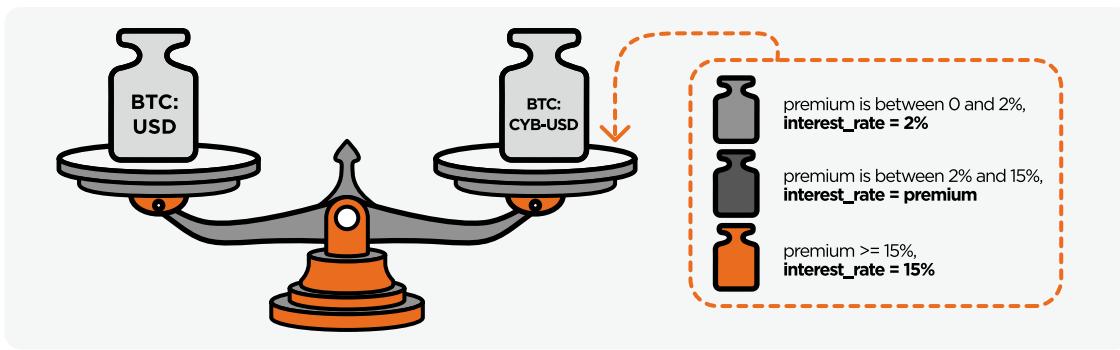


3.4.3 利润激励

拥有 cyb.USD 听上去好像很不错，那么人们为什么要发行它呢？这样做有什么好处呢？这就是利润产生的地方。就每一个被发行出来的 cyb.USD 来说，其持有者都要以一定的利率向发行人付款。可以将它想象成向提供了这种抵押品来缓解市场波动的人支付的费用。

因为 CYBEX 是一个自由市场型的去中心化交易所，1 个 cyb.USD 不一定总是能恰好兑换价值 1 美元的比特币。当这种情况出现时，CYBEX 会调整利率，确保发行人能得到适当的激励来发行更多或更少 cyb.USD，从而实现供求平衡。

例如，如果 cyb.USD 的需求量上升，那么 1 个 cyb.USD 将能兑换价值超过 1 美元的比特币。在这种情况下，我们希望增加 cyb.USD 的供应量，提高利率，使比率重新变回 1:1。反之，我们会降低利率来减少供应量。



按照我们最初的设计，利率将通过以下方式计算：

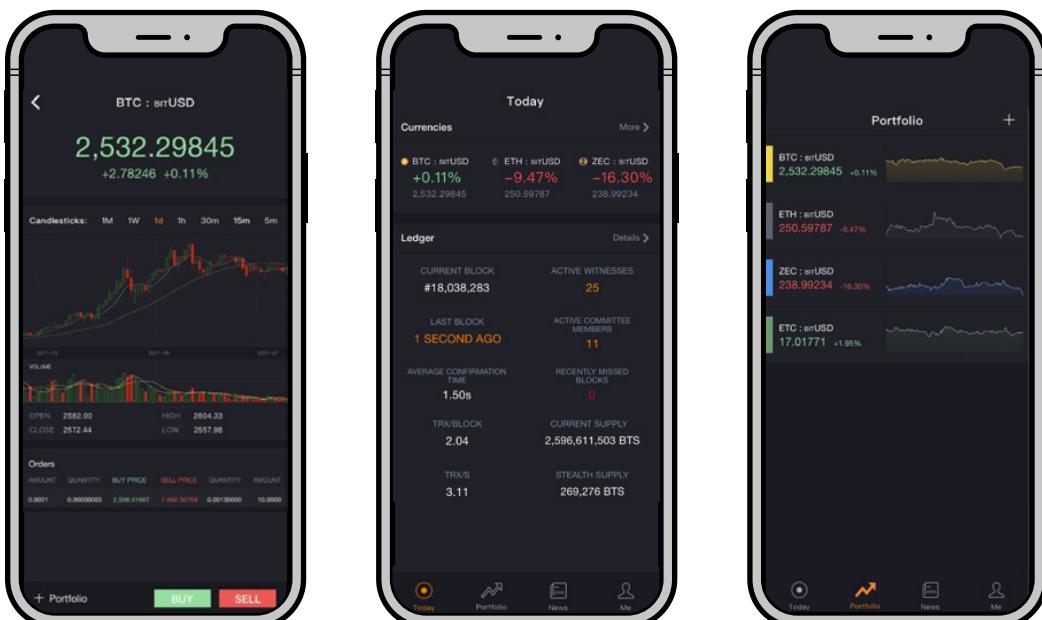
- b_{cyb} = 1个 cyb.USD 在 CYBEX 上能兑换的比特币的数量
- b_{market} = 1美元在主要交易所上能兑换的比特币的数量
- 溢价率 = $(b_{cyb} - b_{market}) / b_{market}$
- 设置利率：
 - 当 (溢价率 < 0) 时, 利率 = 0%
 - 当 (溢价率在 0-2%) 时, 利率 = 2%
 - 当 (溢价率在 2%-15%) 时, 利率 = 溢价率
 - 当 (溢价率 >= 15%) 时, 利率 = 15%

最初的 2% 用来设置一个阈值，以触发发行人的行为——人们往往更容易理解固定的阈值，并且更可能在此基础上采取行动。我们把利率限制在 15% 以内，以确保资产持有者不会因不断上升且可能没有上限的利率感到不安。

然后这个系统会根据 CYBEX 上过去 8 小时内的平均溢价率自动计算利率，然后截屏记录这八小时内 cyb.USD 的总持有量和总发行量。每 8 小时截屏一次，cyb.USD 持有者的账户将被扣除利息（即拥有的 cyb.USD 减少），而发行人的账户将收到相应数额的 cyb.USD。所有的扣款和奖励将依据系统截图进行。

3.5 移动端用户界面

对于任何交易所来说，用户体验都是其取得成功的关键因素。我们将设计移动端和网页界面，确保用户能够进行交易、发行自定义新资产、接收及时信息并使用一些价格稳定资产（如 cyb.USD）进行支付。



3.6 业务拓展

成功运营交易所的一个关键能力在于说服资产持有者在自己的交易所上进行交易。如上文所述，我们在组建 CYBEX 团队前一直在运营 ICOAGE 平台，协助近 40 个来自世界各地的 ICO 项目在中国市场上取得了成功。

以下是我们曾参与的项目的具体信息。但由于 ICO 在中国被取缔，我们已将筹得资金全部归还给投资者。

项目名称	ICO 持续时间
InkChain	2017/8/15 20:00 - 2017/8/16 4:00
CYBEX	2017/7/26 20:00 - 2017/7/26 21:00
Starbase	2017/8/21 10:00 - 2017/8/21 13:00
Indorse	2017/8/29 - 2017/9/3
IPFS	2017/8/3 3:00 - 2017/8/5 14:00
Aeternity	2017/5/29 21:00 - 2017/6/9 21:00
Moed	2017/8/14 14:00 - 2017/8/14 15:00
Hellogold	2017/8/27 14:00 - 2017/8/28 12:00
Encryptotel	2017/4/24 - 2017/5/31
Exscudo	2017/4/25 9:56 - 2017/5/8 18:42
Adel	2017/5/1 - 2017/5/31 23:59
inchain	2017/5/10 - 2017/5/11 10:00
IEX.EC	2017/4/19 - 2017/4/20
Qtum	2017/3/16 - 2017/3/21
WeTrust	2017/3/2 - 2017/4/12
Yoyow	2017/5/21 21:00 - 2017/5/26 21:00
Bitfid	2017/5/12 16:05-2017/5/31 17:54
Storj	2017/5/19 11:00 - 2017/5/25
MobileGo	2017/4/25 10:00 -2017/5/23 19:40
Tenx	2017/6/24 21:00 - 2017/6/24 21:07
Omisego	2017/6/24 13:00 - 2017/6/25 13:00
EOS	2017/6/25 21:00 - 2017/7/2 12:04
Status	2017/6/20 23:30 - 2017/6/21 23:30
Poet	2017/8/8 20:00 - 2017/8/9 10:08
Energo	2017/7/25 18:00 - 2017/7/31 11:50
Genaro	2017/8/15 14:00 - 2017/8/15 14:10
Vechain	2017/8/12 12:00 - 2017/8/12 12:10
Delphy	2017/8/16 18:00 - 2017/8/17 14:00
Primas	2017/8/7 20:00 - 2017/8/14 19:30
Tierion	2017/7/27 21:00 - 2017/7/28 20:00
Gnosis	2017/4/24 - 2017/4/25
Aragon	2017/5/17 - 2017/5/18
Creativechain	2017/4/30 18:21 - 2017/4/30 22:00
TAAS	2017/3/27 - 2017/4/27
KyberNetwork	2017/9/15-2017/9/17

这充分体现了我们不仅能够吸引优秀的项目团队进行合作，而且能在咨询和筹款方面提供有价值的服务。我们将把同样的资源和优势贯彻到 CYBEX 的运营中去。

3.7 主流业务代币化

除了说服已有的区块链项目在CYBEX上交易自己的代币，我们还在积极同更多主流业务部门展开合作，帮助他们实现其当前模式（通常是中心化的）的代币化和去中心化。

由于区块链生态系统仍然是一种比较新的模式，且面临着严重的技术障碍，大部分主流业务仍未开始关注该技术的前景。我们的团队不仅有技术人员，还包括经验丰富的商业和投资专业人士，他们能够利用自己的人脉和专业知识传播区块链的业务潜力，并帮助企业迈出发展的下一步。

下面是几个正在进行中的项目：

- **Talent Token:** 帮助艺术家轻松管理自己的IP并与自己的支持者建立联系，使对中间人的需求最小化。我们正在与日本最大的一家艺人经纪和音乐发布公司合作，将把20多万名歌手、漫画家及演员等艺术家转移到CYBEX 生态系统里的去中心化模式中去。
- **Adspace Token:** 通过消除抽取了大部分利润的中心化平台来帮助内容创作者与广告商直接联系。我们正在与日本最大的广告公司之一合作，将其全年广告收入超过1.34亿美元的内容创作者的全部信息转移到去中心化交易平台上，在交易完成后，广告可以动态嵌入到内容中去。
- **Kickstart Token:** 我们正在与日本最大的众筹平台之一合作，帮助他们开发CYBEX 的副本，来创建一个与CYBEX兼容的众筹生态系统。这种代币有一个托管和投票机制，以确保众筹条款在释放资金前得到满足，所有这些工作都不需要中心化平台。

我们 CYBEX 团队认为，要使区块链变革真正发挥潜力，兑现其去中心化承诺，就必须将更多“主流”业务部门（例如非技术人员能轻易理解的业务）纳入这个生态系统，或者将其“代币化”。

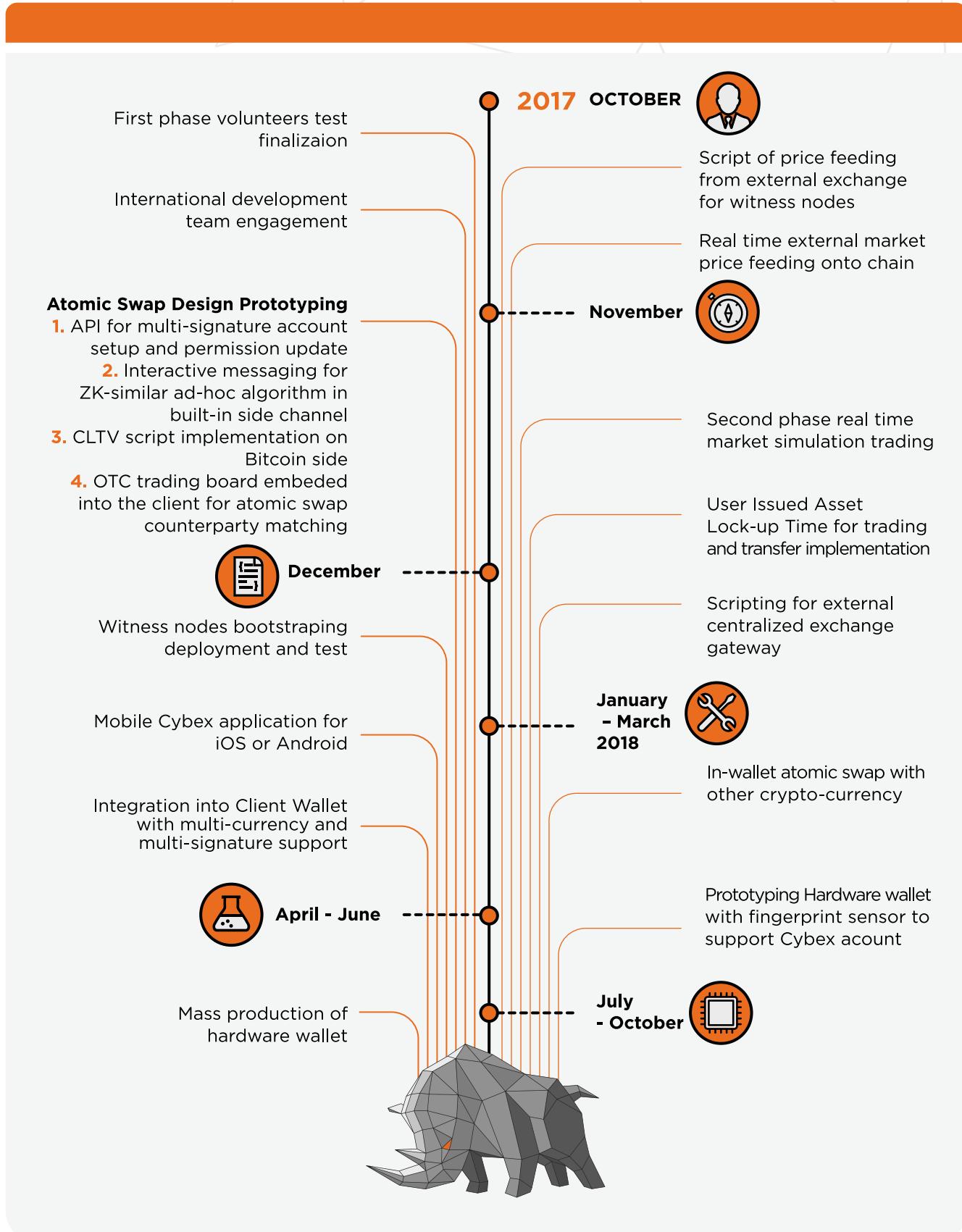
如果您仔细阅读了这篇文章，那么不难发现与我们合作的许多新业务部门本身是中心化平台。我们需要进行大力宣传，而这些平台则需要具备显著的前瞻性与变革意愿，这样才能利用重要资源构建去中心化生态系统，从而有效地淘汰其当前过时的业务模式。

我们还在对许多内容进行探讨，并将继续向社区汇报我们的进展，同时公布新代币的出现及各方参与者。



4. DEVELOPMENT ROADMAP

开发工作路线图



5. THE CYBEX TEAM

CYBEX团队

5.1 核心团队



龚鸣

ICOAGE (曾是中国最大的 ICO 平台) 及区块链铅笔 (最大的中文区块链媒体) 的创始人。2012 年开始致力于推动数字货币和区块链行业的发展，翻译和撰写过大量相关资料和区块链项目白皮书，参与著有《区块链社会》、《区块链——新经济蓝图》、《数字货币》等多部著作。

YURI MILYUTIN

英国伦敦 8760 联合创始人兼市场专家。曾成功帮助以下项目完成 ICO：Populous、AI Gang、Crypto20，募集资金总额超过 8 千万美元。曾担任 UX 顾问、乌克兰基辅 Evoplay 的增长型黑客（Growth Hacker），以及俄罗斯莫斯科 Yandex 公司内部项目 Holibody 的首席执行官兼产品经理。



王坚波

曾任德意志银行 ETF 和中国风险交易总监、花旗中国 ETF 与股权衍生品高级副总裁、瑞信证券股权衍生工具投资副总裁。熟悉全球金融市场及金融衍生品交易，深刻了解全球 ETF 交易以及各类金融创新业务。分别于 2003 年与 2005 年获斯坦福大学电子工程专业学士与硕士学位。

浦志淳

斯坦福大学电子工程硕士，连续创业者及战略顾问，拥有十年以上为 100 强公司提供战略转型咨询与实施服务的经验，目前任德勤副总监，同时也是 LinkSens (IoT 网状网络)、医维博 (供医生交流讨论病例的社交网络) 及 Master He (按摩服务 app) 的联合创始人。



5.2 顾问团队

ASH HAN

Cosmos & Finector 联合创始人，Cosmos 是一个区块链项目，其愿景是“区块链互联网”，Finector 是韩国一家大型区块链／DLT 咨询公司，其客户包括 300 多家政府机构、银行、金融机构等，还有 700 多位个人客户。Han 是一位天使投资人、顾问、社区组织者、作家和公众演讲人，对区块链经济和技术有深入理解，自 2012 年开始投身区块链行业。



李国权

新加坡新跃社科大学教授，毕业于伦敦政治经济学院，计量经济学和数学经济学博士。他作为亚洲 REITS 行业的先驱，创立了自己的对冲基金公司，还是两家新加坡上市公司的独立董事，并且是两个慈善组织的投资委员会和理事会以及新加坡经济学会的成员。曾担任另类资产投资管理协会（新加坡分会）的创始副主席。

谷家衛

毕业于东京大学法学部，随后加入所罗门兄弟，担任亚洲投资部总经理，拥有广泛的投资经验，联合创办了多家基金公司，包括 Tudor Capital Japan, Asuka Asset Management 和 StormHarbour。他还是东京都知事小池百合子的高级顾问以及东京区块链加速器项目“Blockchain Business Camp Tokyo ”的核心架构师之一。



戴有造

斯坦福大学管理科学与工程学士，拥有丰富的企业管理与投资经验，跨境（中国-日本）投资基金公司 Leland Capital 的联合创始人及首席执行官，曾是物流供应商 Yixing SCM 的首席运营官／信息官、埃森哲顾问及多家公司的联合创始人，也是比特币和以太坊的早期中国投资者。

BUDORIN DYMTRIO

Hacken 的联合创始人 - 一个为白帽黑客设计的程序错误悬赏市场。Budorin 曾是德勤审计部门的高级经理，以他的审计大数据解决方案获取了德勤的独立国家联合体 (CIS) 审计挑战竞赛。在乌克兰政府 2014 年的大规模改革后，Budorin 成为了乌克兰军工与国防行业内的一位领先企业家。



6. RISKS

风险提示

加密资产是一种相对较新的资产类别，并具有相当大的投资风险。潜在投资者需充分了解这些风险，并根据各自的风险承受水平进行投资。

以下条款中，根据新加坡法律注册成立的 Cybex System Pte. Ltd. 被称为“出售方”。投资 CYB 的个人或机构被称为“买方”。

a) 信息披露不完备的风险

截至本白皮书发布之日，CYBEX 仍处于开发阶段，其哲学理念、共识机制、算法、代码等技术规范和参数可能会经常且不断更新与变更。尽管本白皮书包含 CYBEX 的特定信息，但其并不绝对完整，且出售方可能会根据特定目的不时对这些信息作出调整与更新。出售方无法，也无义务随时告知参与者 CYBEX 开发中的每个细节（包括其进度和预期里程碑，无论是否推迟），因此并不必然会让参与者及时且充分地获悉 Cybex 开发中不时产生的信息。信息披露的不充分是不可避免且合乎情理的。

b) 监管风险

加密货币正在被或可能被各个不同国家的监管机构所监管。出售方可能会不时收到来自于一个或多个监管的询问、通知、警告、命令或裁定，甚至可能被勒令暂停或终止任何与本次公开售卖、Cybex 开发或 CYB 相关的行动。Cybex 的开发、营销、宣传或其他方面以及本次公开售卖均可能会因此受到严重影响、阻碍或被终结。由于监管政策随时可能变化，任何国家之中现有的对于 Cybex 或本次公开售卖的监管许可或容忍可能只是暂时的。在各个不同国家，CYB 可能随时被定义为虚拟商品、数字资产甚至是证券或货币，因此在某些国家之中按当地监管要求，CYB 可能被禁止交易或持有。

c) 密码学加速发展的风险

密码学正在不断演化，其无法保证任何时候绝对的安全性。密码学的进步（例如密码破解）或者技术进步（例如量子计算机的发明 / 改良）可能给基于密码学的系统（包括 CYBEX）带来危险。这可能导致任何人持有的 CYB 被盗、失窃、消失、毁灭或贬值。在合理范围内，项目方将自我准备采取预防或补救措施，升级 CYBEX 的底层协议以应对密码学的任何进步，以及在适当的情况下纳入新的合理安全措施。密码学和安全创新的未来是无法预见的，项目方将和 CYBEX 社区其他成员一起尝试适应密码学和安全领域的不断变化。

d) 项目失败或中止的风险

CYBEX 仍在开发阶段，而非已准备推出的成品。由于 CYBEX 系统的技术复杂性，出售方可能不时会面临无法预测和 / 或无法克服的困难。因此，CYBEX 的开发可能会由于任何原因而在任何时候失败或中止（例如由于缺乏资金）。开发失败或中止将导致 CYB 代币无法交付给本次公开售卖的任何参与者。

e) 众筹收入被盗的风险

可能会有人企图盗窃出售方所收到的众筹资金（包括已转换成法币的部分）。该等盗窃或盗窃企图可能会影响出售方为 Cybex 开发提供资金的能力。尽管出售方将会采取最尖端的技术方案保护众筹资金的安全，某些网络盗窃仍很难被彻底阻止。

f) 源代码漏洞风险

无人能保证 CYBEX 的源代码完全无瑕疵。代码可能有某些瑕疵、错误、缺陷和漏洞，这可能使得用户无法使用特定功能、暴露用户的信息或产生其他问题。如果确有此类瑕疵，将损害 CYBEX 的可用性、稳定性和 / 或安全性，并因此对 CYB 的价值造成负面影响。开放源代码以透明为根本，以促进源自于社区的对代码的鉴定和问题解决。出售方将与 CYBEX 社区紧密合作，今后持续改进、优化和完善 CYBEX 的源代码。

g) 无准入许可、去中心化自治账本的风险

在当代区块链项目中，有三种流行的分布式账本种类，即：无准入许可的账本、联盟型账本和私有账本。Cybex 底层的分布式账本是无准入许可的，这意味着它可被所有人自由访问和使用，而不受准入限制。尽管 Cybex 初始时是由出售方所开发，但它并非由出售方所有拥有、运营或控制。自发形成的 Cybex 社区是完全开放、去中心化且无准入门槛即可加入的，其由全球范围内的用户、粉丝、开发者、CYB 持有人和其他参与者组成，这些人大都与出售方无任何关系。就 Cybex 的维护、治理乃至进化而言，该社区将是去中心化且自治的。而出售方仅仅是社区内与其他人地位平等的一个活跃成员而已，并无至高无上或专断性的权力，不考虑其之前曾对 Cybex 的诞生做出的努力和贡献。因此，Cybex 在启动之后，其如何治理乃至进化将不受到出售方的支配。

h) 源代码升级风险

Cybex 的源代码是开源的且可能被 Cybex 社区任何成员不时升级、修正、修改或更改。任何人均无法预料或保证某项升级、修正、修改或更改的准确结果。因此，任何升级、修正、修改或更改可能导致无法预料或非预期的结果，从而对 Cybex 的运行或 CYB 的价值造成重大不利影响。

i) 安全漏洞风险

Cybex 区块链基于开源软件并且是无准入许可的分布式账本。尽管出售方努力维护 Cybex 系统安全，任何人均有可能故意或无意地将弱点或缺陷带入 Cybex 的核心基础设施要素之中，对这些弱点或缺陷出售方可能恰好无法通过其采用的安全措施预防或弥补。这可能最终导致参与者的 CYB 或其他数字货币丢失。

j) “分布式拒绝服务”攻击

Cybex 被设计为公开且无准入许可的账本。因此，Cybex 可能会不时遭受“分布式拒绝服务”的网络攻击。这种攻击将使 Cybex 系统遭受负面影响、停滞或瘫痪，并因此导致在此之上的交易被延迟写入或记入 Cybex 区块链的区块之中，或甚至暂时无法执行。

k) 节点处理能力不足的风险

Cybex 的快速发展将伴随着交易量的陡增及对处理能力的需求。若处理能力的需求超过 Cybex 区块链网络内届时节点所能提供的负载，则 Cybex 网络可能会瘫痪和 / 或停滞，且可能会产生诸如“双重花费”的欺诈或虚假交易。在最坏情况下，任何人持有的 CYB 可能会丢失，Cybex 区块链回滚或甚至硬分叉可能会被触发。这些事件的后果将损害 Cybex 的可使用性、稳定性和安全性以及 CYB 的价值。

l) CYB 代币未经授权被认领的风险

任何通过解密或破解 CYB 购买者的密码而获得购买者注册邮箱或注册账号访问权限的人士，将能够恶意认领在本次公开售卖中所购买的 CYB。据此，购买者在本次公开售卖中所购买的 CYB 可能会被错误发送至通过购买者注册邮箱或注册账号认领 CYB 的任何人士，而这种发送是不可撤销、不可逆转的。每一购买者应当采取诸如以下的措施妥善维护其注册邮箱或注册账号的安全性：
(i) 使用高安全性密码；(ii) 不打开或回复任何欺诈邮件；以及 (iii) 严格保密其机密或个人信息。

m) CYB 钱包私钥丢失风险

若丢失或损毁了存取 CYB 所必需的私钥，这可能是不可逆转的。只有通过本地或在线 CYB 钱包来占有相关的独一无二公钥和私钥，才可以操控 CYB。每一购买者应当妥善保管其 CYB 钱包的私钥。若 CYB 购买者的该等私钥丢失、遗失、泄露、毁损或被危及到，出售方或任何其他人士均无法帮助购买者存取或取回相关 CYB。

n) 系统分叉风险

Cybex 是一个由出售方发起并由社区提供支持的开源项目。尽管出售方在 Cybex 社区中具有影响力，但是其并不也无法独断 Cybex 的开发、营销、运行或其他。任何人士均可以开发 Cybex 代码的补丁或升级，而无需获得任何其他人士的授权。一旦部分的 Cybex 区块链上验证者接受 Cybex 的补丁或升级，这可能导致 Cybex 区块链“分叉”，由此将会有两条分叉的网络，直至分叉的区块链合并或者其中某一条终止出块（这两种情况可能永不会发生）。Cybex 区块链由于分叉而产生的每一分支均将有其自己的加密代币。因此，在两条分叉的分支上会分别存在拥有几乎相同技术特征和功能的 CYB。Cybex 社区可能分裂成两批，分别支持两条分支。此外，分叉出的 Cybex 区块链分支在理论上可以进一步无限次分叉。分叉区块链的暂时性或永久性存在可能对 Cybex 运行及 CYB 的价值造成不利影响。在最坏情况下，可能摧毁 Cybex 系统的可持续性。尽管 Cybex 区块链上的该等分叉有可能经社区牵头努力后将两条分支合并而解决，但并不能保证成功且可能耗时很久。

o) 代币通胀的风险

取决于 Cybex 发布时的具体底层协议，CYB 总量可能随时间略有增加，且可能会由于采纳了 Cybex 源代码的补丁或升级而进一步增加。由此产生的 CYB 供应量通胀可能导致市场价格下跌，从而 CYB 持有者可能遭受经济损失。CYB 购买者或持有者并不能被保证会由于 CYB 通胀而获得某种形式的赔偿或补偿。

p) 平台合并的风险

技术角度而言，在特定情形下，为实现协同效应或基于其他有价值的对价，Cybex 可能与其他区块链项目合并。这种形式的合并可能导致 Cybex 区块链被放弃或废弃，以换取新创建的其他区块链上一定数量的加密代币。该等新的加密代币将按一定兑换率分配并派发给合并前的 CYB 持有者。在特定估值模型下 CYB 持有者可能在该等合并中获得的补偿不足。

q) 应用缺少关注度的风险

CYB 的价值很大程度上取决于 Cybex 平台的普及度。Cybex 并不预期在发行后的很短时间内就广受欢迎、盛行或被普遍使用。在最坏情况下，Cybex 甚至可能被长期边缘化，仅吸引很小一批使用者。相比之下，很大一部 CYB 需求可能具有投机性质。缺乏用户可能导致 CYB 市场价格波动大从而影响 Cybex 的长期发展。出现这种价格波动时，出售方不会（也没有责任）稳定或影响 CYB 的市场价格。

r) 流动性不足风险

CYB 既不是任何个人、实体、中央银行或国家、超国家或准国家组织发行的货币，也没有任何硬资产或其他信用所支持。CYB 在市场上的流通和交易并不是出售方的职责或追求。CYB 的交易仅基于相关市场参与者对其价值达成的共识。任何人士均无义务从 CYB 持有者处兑换或购买任何 CYB，也没有任何人士能够在任何程度上保证任何时刻 CYB 的流通性或市场价格。CYB 持有者若要转让 CYB，该 CYB 持有者需寻找一名或多名为有意按约定价格购买的买家。该过程可能花费甚巨、耗时长并且最终可能并不成功。此外，可能没有加密代币交易所或其他市场上线 CYB 供公开交易。

s) 代币价格波动风险

若在公开市场上交易，加密代币通常价格波动剧烈。短期内价格震荡经常发生，该价格可能以比特币、以太币、美元或其他法币计价。这种价格波动可能由于市场力量（包括投机买卖）、监管政策变化、技术革新、交易所的可获得性以及其他客观因素造成，这种波动也反映了供需平衡的变化。无论是否存在 CYB 交易的二级市场，出售方对任何二级市场的 CYB 交易不承担责任。因此，出售方没有义务稳定 CYB 的价格波动，且对此也并不关心。CYB 交易价格所涉风险需由 CYB 交易者自行承担。

t) 竞争风险

Cybex 的底层协议是基于开源电脑软件，没有任何人士主张对该源代码的版权或其他知识产权权利。因此，任何人均可合法拷贝、复制、重制、设计、修改、升级、改进、重新编码、重新编程或以其他方式利用 Cybex 的源代码和 / 或底层协议，以试图开发具有竞争性的协议、软件、系统、虚拟平台或虚拟机从而与 Cybex 竞争，或甚至赶超或取代 Cybex。出售方对此无法控制。此外，已经存在并且还将会有许多竞争性的以区块链为基础的平台（例如 BitShareess）与 Cybex 产生竞争关系。出售方在任何情况下均不可能消除、防止、限制或降低这种旨在与 Cybex 竞争或取代 Cybex 的竞争性努力。

u) 第三方开发者风险

Cybex 将提供一个开放平台适用于第三方（尤其是 Cybex 社区成员）开发的任何类型的分布式应用和智能合约程序。所有这些应用和智能合约程序可以被接入或建立在 Cybex 区块链上而不受限于审查制度、限制、控制、资格预审或准入要求。出售方既不意图也无法担当审查员在任何程度上对任何将要在 Cybex 系统上开发或与之相关的程序进行审核。因此，在特定司法管辖区域被禁止或限制的程序，如涉及赌博、投注、彩票、乐透、色情等等的程序，可能利用 Cybex 区块链的无准入要求来开发、促进、营销或运营。特定司法管辖区域的监管当局可能对特定程序或甚至其开发者或用户采取相应行政或司法措施。任何政府当局的处罚、惩罚、制裁、镇压或其他监管措施，或多或少会惊吓或威慑到既有或潜在 Cybex 用户使用 Cybex 系统并持有 CYB，从而对 Cybex 的前景造成重大不利影响。

v) 平台迁移风险

Cybex 初始时将有一条独立的底层区块链作为其自有账本。然后 Cybex 今后可能迁移去其他一个或多个分布式平台，只要该等平台对 Cybex 上执行的交易更高效、更有价值或更适合。若发生该等迁移，所有届时存在的 CYB 将能被转换成迁移后的 Cybex 上新的内置加密代币，其具有类似或同等技术规格和功能。Cybex 在迁移前使用的原区块链将因此渐渐消亡。

w) 其他加密资产的风险

Cybex 中将会创建或生产并流通着各种加密资产。这些加密资产中一部分可能是由特定人士发行的，发行人将对持有人负有特定承诺或义务。其他一些加密资产可能是由 Cybex 内的智能合约创建的。这些加密资产都不会带有和 CYB 一样或类似的功能。这些加密资产既不是出售方所出售或提供的，出售方也不会对它们负责，除非出售方另有特别说明。