



白皮书

2018



# 目录

重要提示 .....	4
1. 介绍 .....	6
2. 行业概况 .....	8
1) 全球金融机构支付系统- 蓝天市场 .....	8
2) 现行资金转账过程如何运作 .....	9
3) 现行资金转移中的信息 .....	11
4) 行业监管 .....	11
a. 金融机构反洗钱 ("AML") .....	11
b. 反洗钱法的分析 .....	12
c. 更多信息的好处 .....	12
3. ivyKoin机会 - 高度颠覆性的先进技术 .....	13
1) 与现行金融系统的比较 .....	13
2) 与竞争加密货币的比较 .....	15
4. 我们的世界级一流团队拥有成功的记录 .....	17
5. ivyKoin运营明细 .....	18
1) 运营平台概况 .....	18
a. 基本功能 .....	18
b. 对等加密货币到法定货币网络 .....	18
c. 软件集成 .....	18
d. 收银和转换服务 .....	18
e. 通过公开市场操作的固定价格转移 .....	19
2) 金融机构 .....	19
3) 用户功能 .....	19
a. 账户开设和管理 .....	20
i. 发送人数据验证 .....	20
b. 交易管理 .....	20
c. ivyKoin购买, 销售和转账 .....	20
6. ivyKoin 技术规格 .....	22
1) 技术架构概述 .....	22
a. 公共网络, ivySend, 公共ivyKoin代币 (IVYA) .....	24
b. 私人网络, ivyReceive和私人 ivyKoin 代币 (IVYB) .....	24
c. 跨链通讯和 ivyKoin Oracle服务 .....	25
2) ivyKoin网络上的身份 .....	26
a. 发送人身份 .....	26
b. 金融机构和中间机构身份 .....	26
3) 区块链技术应用 .....	26
4) ivyKoin 数据容器 .....	28
a. 数据容器的生成与存储 .....	29
b. 访问ivyKoin数据容器 .....	29
7. 代币生成事件后代币结构 .....	30
8. 路线图 .....	32
a. 代币 .....	32
b. 操作 .....	32
10. 风险 .....	34
词汇 .....	37

# 重要提示

本文档是一份技术白皮书，介绍了ivyKoin技术当前和未来的发展。本文件不是披露文件。本文件专供接收方（**接收人**）用于通过按照Ivy Koin LLC (**ivyKoin**或公司)发行的预售承诺函授予的代币权利（**权利**），考量购买代币（**代币**）的机会（**如后文所述**）。

本文档中包含的任何信息，或随后代表公司或其各自雇员，代理人或顾问口头或书面提供给接收人的信息均按照本文件所述条款和条件提供给接受方。

本文件为保密文件，未经本公司事先书面同意，不得以任何形式复制或传播给其他任何人。

通过保留此文件，接收人承认并向公司表示已阅读，理解并接受本文件条款。如果接收人不接受这些条款，则必须立即此文件退回给公司。

本文件仅为传达信息目的及协助接收人决定是否进一步调查可能获得权利和代币的机会，并且仅可用于此目的。本文件日期为2018年1月16日，由公司根据当时可用信息发布和制作。

本文件并非意图提供任何投资或信用决策或任何其他风险评估的唯一或主要依据。任何接收人都应根据其认为必要或可取的独立调查来确定其获取权利和代币的权益。

尽管公司在编制本文件时已经采取了应有的注意和尽职调查，但本公司或其任何顾问并不就本文件资料的准确性或完整性作出任何声明或保证。本文件中包含的任何信息或向接收人传输或提供的任何其他书面或口头通讯均不得作为可供接收人依赖的承诺或声明，且公司对此文件中任何估计，预测或预期的准确性或可实现性均不作出任何陈述或保证。对于任何此类信息，估计，预测或预期，本公司或其顾问概不负责。  
本文件尚未并将不会提交给澳大利亚证券和投资委员会（**ASIC**）。本文件的目的仅为接收人提供信息，并不构成2001公司法（Cth）（**公司法**）或其他司法管辖区的任何同等立法中所定义或提及的招股说明书，简易招股说明书或其他披露文件。

潜在的权利和代币购买者应阅读本文件的全部内容。如果您在阅读本文件后有任何疑问，请联系向您提供此文件的人员。本公司保留全权决定是否向任何人士出售权利或代币的权利。

## 责任免除

对于由于与此文件任何方式相关原因，包括但不限于本文件中包含的信息，任何错误或遗漏，或其准确性或可靠性，而导致（包括疏忽）使接收人或任何其他人员或实体遭受或产生的任何损失或损害，公司均不承担任何责任。

## 免责声明

本文件仅供参考。本文件中的信息可能并不完整，可能会在任何时候被公司更改，修改或修订，并不意图也不构成公司的声明和保证。此外，公司可不限以任何其认为合适的方式使用权利及代币出售所筹集的资金。

公司或公司的任何其他顾问均不意图更新本文件或接受任何义务向接收人提供信息的访问权限或增加任何其他信息，或更正文件中或可获得的关于公司、权利或代币的其他任何其他信息中出现的不准确之处。

公司业务最近刚刚形成，是一家“创业企业”，没有任何显著的经营历史可作为依据来对其业务和前景以及代币的发展前景进行评估。因此，这里所包含的信息本身就属于推测性质。



## 无推荐意见

本文件不代表购买权利或代币的建议。任何购买权利或代币的决定必须基于拟购买者自身情况，调查，分析和对公司运营和前景以及权利和代币的评估。潜在购买者必须自行独立评估购买权利和代币的好处，并咨询自己的专业顾问，在认为必要时进行进一步调查。潜在购买者会注意，任何权利或代币的购买都可能涉及高度的风险。

根据《公司法》第766B条的规定，本文件中的任何内容都不应解释为个人或一般的金融产品建议。本文件不涉及或暗示对是否购买，出售或持有金融产品的建议或意见陈述。

## 税收

购买权利或代币将产生税收后果，情况因每个权利或代币购买者的个人财务状况而异。我们要求所有潜在的权利或代币购买者从税收角度和一般情况获得有关购买权利和代币的后果的独立财务建议。在法律允许的最大范围内，公司，公司高级管理人员及其各自的顾问不承担购买权利或代币税收后果的责任和义务。

## 美元

除非另有说明，否则所有货币金额均以美元为单位。

## 合格声明

本文件包括“预测”，“计划”，“针对”，“认为”，“潜在”，“估计”，“意图”和“目标”等术语。这些陈述是基于当前对公司业务的理解以及业务所抱有的期望目标。但是，应该指出，实现这些陈述存在固有风险，潜在的购买者在购买权利或代币时应以这些目标可能不会实现为基础。

## 代币使用

公司建议建立数字平台来使用代币，该数字平台还将用于支付（**ivyKoin**网络）。

如果实施，代币持有者可以自愿地将交易数据取消匿名直到金融机构满意，以便在利用加密货币促进交易的同时具备区块链的安全性和可靠性。



# 介绍

加密货币市场正在迅速扩大和深化，目前加密货币市场资本总额为720亿美元。<sup>1</sup>



虽然这些货币的优势和潜力得到了广泛认可，但匿名却导致缺少支持涉及加密货币交易的金融机构，进而阻止了其更主流的接受度。

全球银行业和金融业缺乏支持的主要原因是由于适用法规要求的某些交易信息与匿名性产生了冲突。

代币将是一个基于区块链的加密货币，意图与金融机构进行交易，与现行支付网络（包括目前的基准支付系统，如SWIFT协议，CHIPS和Fedwire）相比，嵌入了更多的了解交易（KYT）和了解客户（KYC）信息。

代币持有者将有能力自愿地对交易数据进行去匿名化处理，直到金融机构满意，从而利用区块链的安全性和可靠性促进使用加密货币的交易。

我们相信代币的机会是巨大的，因为有：

- 蓝天市场
  - 潜在的加密货币市场持续增长
  - 全球金融机构交易的潜在渗透
- 我们的高度颠覆性技术
  - 与我们最相近的同行Ripple和全球领先的Altcoin的相比，IvyKoin网络预计会有架构上的改进。目前，Ripple的市值约为1240亿美元<sup>2</sup>。
- 我们的世界级一流团队，有交付历史记录

我们在下面详细列出我们的建议，并期待您能成为一个代币持有者。

**Ivy Management Group LLC**

2018年1月16日

- 
1. <https://coinmarketcap.com/> 2018年1月9日
  2. <https://coinmarketcap.com/> 2018年1月7日



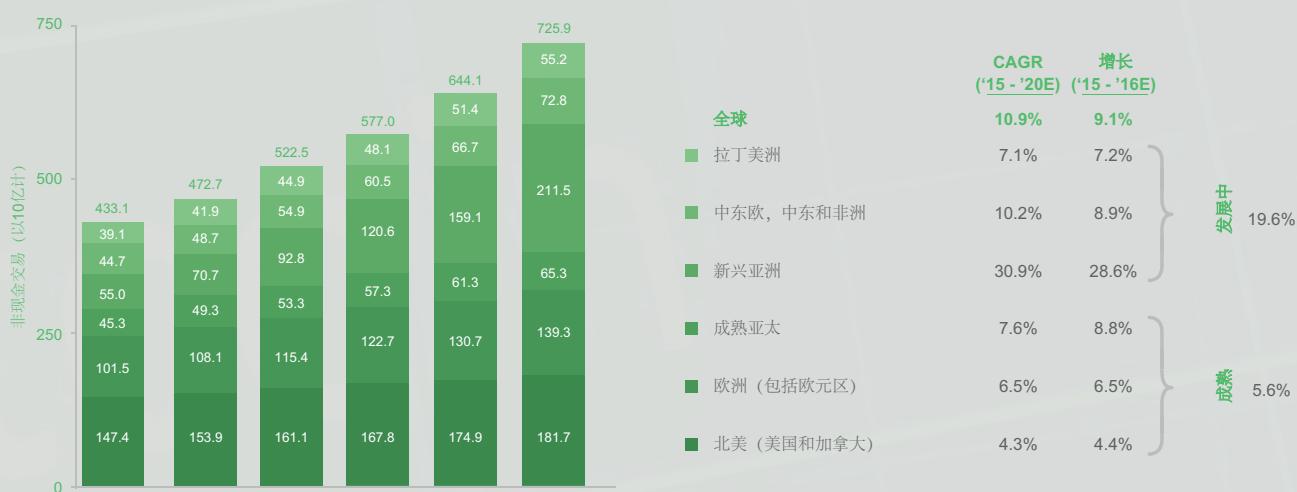
# 行业概况

## 1) 全球金融机构支付系统 - 蓝天市场

全球金融机构支付意义重大。我们的SWIFT平台每天指导全球转移转账近5万亿美元，即每年1250万亿美元<sup>3</sup>。

下面的图表也显示了该行业的同比增长。表格揭示了新兴市场支付的增长速度，但是在北美和欧洲等更为成熟的地区，基于加密货币的支付解决方案存在着更大的可立即打开的市场。

Figure 2 –2017年世界支付报告<sup>4</sup>



3. [https://www.fincen.gov/sites/default/files/shared/Appendix\\_D.pdf](https://www.fincen.gov/sites/default/files/shared/Appendix_D.pdf)  
4. Capgemini & Royal Bank of Scotland 2017

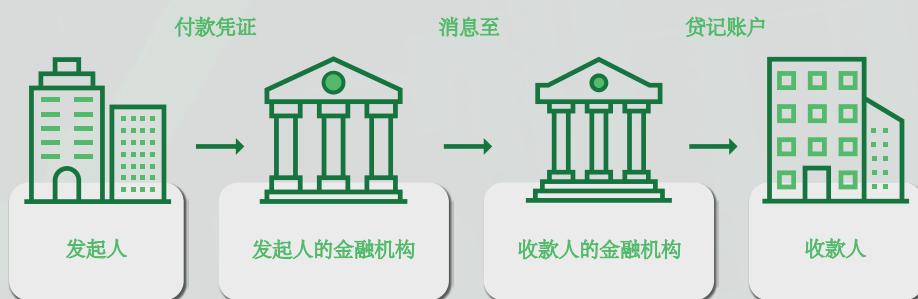
## 2) 现行资金转账过程如何运作

电子资金转账是在金融机构客户的指示下，将金钱从一个金融机构转移到另一个金融机构（或从一个账户转移到另一个账户）的交易。金融机构通过电子信息的交流实现了这一点，这些信息构成了进行必要的记账条目和提供资金的基础。电子资金转账是企业用来在双方间转移资金的主要形式。

金融机构按照通用和有良好基础的标准通过收发电子消息来实现电子资金转账，标准包括SWIFT和ISO 20022。金融机构之间发送的信息指示发送银行借记发送方账户，收款银行贷记收款方账户。

参与转账的实体包括：

- 发起者（如企业或个人）——转账发起人；
- 收款人——转账的最终接收方；
- 发起人的金融机构——接收发起人转账指令的金融机构，并将资金转移到收款人的金融机构；
- 收款人的金融机构——接收资金并持有贷记账户的金融机构；和
- 其他/中间金融机构——可能需要执行交易的其他机构。



常用的支付形式包括：

<b>SWIFT</b>	<p>全球银行间金融电信协会（简称“<b>SWIFT</b>”）是成员所有制的信息网络，用于使用标准化代码的资金转账指令。</p> <p>SWIFT是一个通信网络，一个国家的金融机构可以用它与其他国家的分支机构或其他金融机构进行通信。 SWIFT是一种用于资金转账指令的通讯系统，而不是一个财务结算系统。</p> <p>大多数国际银行间信息都使用SWIFT网络。 SWIFT将其消息分成一系列格式，称为消息类型。每种消息类型表示一种交易或消息。消息类型分为十类：（MT0xx - 系统消息； MT1xx - 客户支付和支票； MT2xx - 金融机构转账； MT3xx - 国债市场； MT4xx - 收款和现金运送单； MT5xx - 证券市场； MT6xx - 国债市场 - 金属和联合企业； MT7xx - 跟单信用证和担保； MT8xx - 旅行支票； 以及MT9xx - 现金管理和客户状态）。</p> <p>SWIFT平均每天记录2,840万条FIN消息<sup>5</sup>。 SWIFT每天在全球转账近5万亿美元，即每年1250万亿美元<sup>6</sup>。</p>
<b>CHIPS</b>	<p>结算所银行间支付系统（“<b>CHIPS</b>”）是一种资金转账系统，为世界上一些规模最大、最活跃的银行传输和结算美元付款订单。</p> <p>CHIPS平均每天传输和结算价值1.5万亿美元的446,000多条“付款消息”。它每天运行20个小时，并实时匹配银行间的交易<sup>7</sup>。</p>
<b>Fedwire</b>	<p>Fedwire资金服务（“<b>Fedwire</b>”）是由12家美国联邦储备银行共同拥有的实时全面结算系统<sup>8</sup>。付款人和收款人都必须在参与Fedwire的金融机构开立账户，转账是当天不可撤销的付款。虽然参与机构都是美国的机构，但Fedwire可以用于国际转账中的美国的部分。</p> <p>2016年，Fedwire平均每天交易量为590,209笔交易，相当于3.05万亿美元<sup>9</sup>。</p> <p>Fedwire服务于美国东部时间（GMT - 5）工作日前一天晚上9点开始运营至晚上6点。</p>
<b>ACH</b>	<p>自动清算所（“<b>ACH</b>”）是一个由全国自动清算所协会（“<b>NACHA</b>”）运营的电子支付网络，该协会是一个由10,000多家金融机构支持的非营利会员协会。 ACH转账包括直接存款，工资支付和消费支付（例如保险和抵押公司）。</p> <p>ACH直接借记转帐包括消费者支付保险费，抵押贷款和其他类型的账单。 ACH覆盖美国，相当于欧洲的SEPA（单一欧元支付区），英国有三个类似的系统：BACS，CHAPS和Faster Payments。</p> <p>ACH网络每年转移43万亿美元和250亿电子金融交易<sup>10</sup>。</p>

金融机构根据交易的性质使用各种支付形式。在一些情况下，单个交易中可能使用多个支付方法

5. <https://www.swift.com/about-us/swift-fin-traffic-figures> (Date: 19 December 2017)
6. [https://www.fincen.gov/sites/default/files/shared/Appendix\\_D.pdf](https://www.fincen.gov/sites/default/files/shared/Appendix_D.pdf)
7. <https://www.theclearinghouse.org/-/media/tch/pay%20co/chips/reports%20and%20guides/chips%20volume%20through%20november%202017.pdf?la=en> (Date: 19 December 2017)
8. [https://frbservices.org/serviceofferings/fedwire/fedwire\\_funds\\_service.html](https://frbservices.org/serviceofferings/fedwire/fedwire_funds_service.html)
9. [https://www.federalreserve.gov/paymentsystems/fedfunds\\_ann.htm](https://www.federalreserve.gov/paymentsystems/fedfunds_ann.htm)
10. <https://www.nacha.org/ach-network/timeline> (Date: 19 December 2017)

### 3) 现行资金转移过程中的信息

在金融行业，双方之间的交易通常被称为第三方支付。也就是说，是金融机构代表各方（个人或实体）处理交易，而这些个人或实体本身不是金融机构。除了一些主要的例外情况，这些交易通常可以分为两种主要类型：

- 根据金融机构知情的文件处理的交易，例如在贸易融资的情况下，一个或多个金融机构可以获得信用证，担保和/或其他一些信息，如提货单和其他运输信息。
- 没有拥有此类文件的金融机构参与的交易。这些交易通常被称为“单纯支付”。绝大部分第三方支付都属于这种类型，在这种情况下，处理付款的金融机构对相关交易的性质的可见度相对较低。在贸易融资领域，这种交易被称为“记账交易”。

可能包含在金融交易中的信息分为两类：

- 了解客户（KYC）：KYC信息通常包括身份信息，如客户的姓名，地址，账号等。
- 了解交易（KYT）：KYT信息包括交易类型（例如，交易是否涉及现金，外国电汇付款或支票）和资金的收款人（包括付款人在指示时报告的地址）详细信息以及交易记录中包含的细节。

### 4) 行业监管与ivyKoin的相关性

在过去的50年中，资金转移越来越电子化。随着这种进步，以及随之而来的交易量的增加，金融机构、执法机构和监管机构面临着越来越多的打击金融犯罪的复杂挑战。世界各地的司法管辖区继续强化反洗钱（AML）法律。由于几乎所有国家都已采用并投入越来越多的资源来执行这些类型的法律，消费者和企业习惯于金融机构要求提供KYC信息以便在开立新的金融账户或经手大额资金转移的时候验证客户的身份。

#### a. 金融机构反洗钱

以美国为例，《银行保密法》<sup>11</sup>和其他规定要求金融机构执行和遵守能够充分察觉、调查和报告可疑活动的政策、程序和控制措施。这包括可能代表洗钱，逃税或其他犯罪活动的交易。在世界各地的发达经济体中，类似的要求也很普遍。

用于查探可疑活动的方法通常涉及按批量审查客户最近活动的基于规则的自动化可疑活动监视平台。这些规则或情景会标记特定交易或交易组，以供进一步分析。这种分析通常需要金融机构人员进行人工审查，进而将被标记的活动确认为“不可疑”，或将活动升级以供进一步审查，并可能随后向执法机构报告。

此外，某些高风险客户经常受到定期进行的尽职调查评估，这些评估涉及对客户在一段时间内（例如最近6个月或12个月）进行的交易的深度分析。这些尽职调查审查与自动化交易监控检测方法具有相似的目的，即了解相关活动的性质，这样金融机构可以就保留客户关系的风险和可接受性做出决策，对识别方的账户进行适当控制，并根据需要报告可疑活动。

对这一领域的监管预期是，金融机构能够进行充分的尽职调查和分析，以确认客户活动并不可疑，如有可疑则对该活动进一步分析并向执法部门报告。金融机构应根据所有可用信息进行这些评估；如果有更多的信息可以提供帮助，那么金融机构需要收集这些信息，但采取的方式不应“惊动”任何人——包括客户或相关方——使之察觉调查已经，或可能正在进行。

11. <https://www.occ.treas.gov/topics/compliance-bsa/bsa/index-bsa.html>



### **b. 反洗钱法的分歧**

遵守反洗钱法要求银行有足够的信息来促进，执行和支持其异常检测计划。加密货币及其固有的匿名性使银行处于一种约束状态，因为这些交易并非自然伴随着银行实施他们识别欺诈或非法活动所需的信息。为了保护自己，银行通常暂停含有源自加密货币相关交易的法定存款的账户，并拒绝接受加密货币作为合法交易媒介产生的收益或结算。这个决定的一个含义是，合法的企业无法从事涉及加密货币的交易，因为他们无法存入收益。

### **c. 更多信息的好处**

无论是调查自动化交易监控系统的警报时，还是在作为持续尽职调查一部分的活动评估期间，获得更多随时可用的信息可以带来明显的好处。额外信息可以帮助调查人员或审查员更有效地确定活动性质（包括相关方）的适当性或合法性是否值得怀疑。

这些额外信息可以帮助金融机构确定客户是否需要被归类为高风险，或者该机构是否违反了反洗钱法规定的义务。在日常的良性活动中，这些信息可以让银行更有效地将调查资源集中在其他客户和他们的高风险活动上。

尽管传统的支付方式通常嵌入了有限的信息，但这些附加数据通常可以在金融机构关于指导客户的KYC记录中获得，或者由客户直接在交易指令中提供。

前一种类型的信息可以包括例如客户业务性质的描述，其地理中心，账户可能经历的预期活动以及关于账户的相关方的信息，诸如收款方的所有者和签署人。交易本身（KYT）可以包括与支持文件相关的信息，例如发票，信用票据，发货文件和交易双方的身份信息（这些可能包括比发起人和收款人以外的各方，例如船运公司）。它还可以包括能够证明交易合法的文件或证明文件的证据，例如由美国财政部外国资产管理办公室或商务部工业和安全局颁发的许可证。

将这些信息作为支持协议的一个方面嵌入到支付指令机制中，对于帮助金融机构的审查人员形成一个关于相关活动性质的更全面和清晰的图景，可能至关重要。通过让KYC和KYT信息更容易获得并消除知识差距，金融机构可以将注意力集中在调查其他应该受到严格审查的情况。遗憾的是，金融技术方面的一些协议发展主要集中在互操作性和速度上，将监管合规性视为会产生不便之处，推迟到部署完成后期阶段予以解决，这意味着很少有实现全面解决方案的承诺。

# 3

## ivyKoin机会 高度颠覆性的先进技术

加密货币的好处**vs** 现行金融系统显而易见



更快



更容易



价格更低



可追踪



无延迟



更多数据



安全

然而，目前大多数加密货币固有的匿名性与当前的金融体系不兼容。

ivyKoin网络将使用基于区块链的加密货币对支持交易的KYC, KYT和AML数据进行捕获。它将主要针对与金融机构的交易，嵌入比现行支付网络更多的合规性和更多交易审计信息。交易数据的提供将满足金融机构和中间机构的严格要求。在实施时，ivyKoin网络将比现行金融系统和竞争的加密货币具有明显的优势。

ivyKoin寻求缩小目前全球金融体系与加密货币的出现之间的差距，将其定位为全球支付的未来。

### 1) 与现行金融系统的比较

在完全开发之后，ivyKoin网络和传统支付网络的主要区别在于ivyKoin网络：

- 通过可信任的分布式ivyKoin网络，在安全实现加密货币付款转账的同时关联KYC和KYT数据
- 将不可变更的参照信息安全存储在公共区块链的交易数据中；
- 比传统的支付方式在转账中嵌入更多的KYT信息；
- 比传统的支付方式在转账中嵌入更多的KYC信息；
- 将能够被集成到现有的银行软件中；
- 易于集成到会计软件中，提高记账效率；
- 向金融机构，会计师，公司经理等根据其要求的信息提供KYC / KYT数据的可撤销访问。



对于KYC和KYT，常用的现行付款形式通常支持收集相对较少的数据点。下表列出了典型交易中包含的KYC / KYT数据点的大致数量：

	<b>SWIFT</b>	<b>Fedwire</b>	<b>Chips</b>	<b>ACH</b>
KYC和AML 数据点	10	17	9	10

注意：本公司不隶属于SWIFT, CHIPS, ACH或Fedwire。所有信息均按一般基础提供，并基于公司研究时的可用信息。

在实施时，ivyKoin网络将比现有的系统和流程更具描述性。根据所执行的金融交易的类型，ivyKoin网络将允许在交易消息中包含超过120个不同的KYT数据点和超过70个不同的KYC数据点。对这些数据点进行分类的一种简单方法是根据它们可能出自的文档来源。



## 2) 与竞争加密货币的比较

代币在充分发展的情况下，将成为一种具有以下几个显着特点和优势的加密货币：

特点	描述	好处
 可识别	ivyKoin网络和相关交易能将KYC / KYT / AML数据清晰整合到加密货币交易流程中。	当事人的和交易的目的合法性很容易理解，并便于用于判决有关付款和存款的决定。
 可转移	代币作为一种加密货币存在，可以在公共区块链上自由交易，而不会阻止金融机构和中间机构所需的相关的KYC / KYT / AML相关信息。	代币的实用性便于各方可以轻松使用和交换，可以诚实反映其价值并取消ivyKoin.com和加密货币作为加密货币价值的唯一决定因素。
 不可伪造	ivyKoin网络交易和支持数据将有助于区块链架构的使用，从而强化分配和交易数据的不变性。	ivyKoin网络的用户将被确保交易完整性和数据安全性，进而确保交易和支持与现金流动有关决定的数据的持久性。
 限量供应	代币将以已知数量发行，并具有已知的初始分布和分配。	公共交易从与钱币稀缺相关的经济中受益，其中私有网络的流动准确反映了网络内货币流动性和流动速度。.
 根据要求去匿名化	所收集的所有数据在由金融机构和中介机构组成的私人清算网络上得到持续的保护，运输和追踪。	符合资格方拥有他们在KYC / KYT / AML功能上所需的信息。在不影响数据的基础安全的情况下，可以添加或移除各方。



ivyKoin网络经充分开发后预计比我们领先的竞争加密货币Ripple具有更显著的优势。



具体来说，相比Ripple，ivyKoin网络是专门的去中心化验证人网络，由金融机构和中间机构组成，他们使用代币来沟通KYC / KYT / AML数据以及在网络上结算余额。合规性和审计是ivyKoin网络的首要关注点。涉及代币的交易将根据公共以太坊网络上列出的合约被发起，使用的代币由于能够实现在金融机构以法定货币向汇款接收人支付款项而可以轻松被交易。这与使用XRP（核心Ripple货币）有很大不同，因为该货币除了作为交易媒介外几乎没有公共用途。

市场潜力得到公认。Ripple是比特币后最大<sup>12</sup>的加密货币之一。



Ripple代币在2017年间增值超过28,000%。

<http://fortune.com/2017/12/29/ripple-cryptocurrency-surge/>

\* 参考日期2018年1月14日

\*\*根据筹集1500万美元计算

12. <https://coinmarketcap.com/> 2018年1月14日

## 我们的世界级一流团队 拥有成功的记录

公司由一支有成功记录的世界级团队领导。公司经验丰富的管理团队还有全球咨询委员会的支持，委员会在所有项目成功所必要的垂直领域拥有无与伦比的行业知识和网络。  
有关团队的信息，请访问 [www.ivykoin.com](http://www.ivykoin.com).



# 5

## ivyKoin 运营明细

### 1) 运营平台概况

#### a. 基本功能

我们对ivyKoin网络的设想是为最终用户提供以下功能。该功能可通过桌面/网页和移动体验传递给其附属成员：

发送人和接收人：

- 购买或出售代币；
- 查看通用加密货币的加密货币兑换可能性和汇率；
- 估计网络费用并接收使用的代币的报价；
- 查看金融机构和金融中间机构平均时间进行交易结算；和
- 查看有关个人身份信息的KYC数据访问日志（针对发送人）

金融机构和金融中间机构

- 维护企业账户和身份信息；
- 管理组织成员的帐户访问设置；和
- 查看代币数据容器内容和访问历史

除上述基本功能外，公司计划在适当的时候将以下特点、功能和解决方案整合到ivyKoin网络中：

#### b. 对等加密货币到法定货币网络

尽管ivyKoin网络的初始用途主要是提供企业对企业的交易，但对能够让个人轻松发送、接收和管理加密货币并轻松将其转换为法定货币的简化的支付网络也存在强大的需求。

#### c. 软件集成

公司将寻求与现有的银行软件集成，以便KYT和KYC在各银行系统内能够自动分配到正确位置。

公司还打算与主要会计软件系统集成。客户的支付和收据（包括发票详细信息）的轻松集成将使交易数据可以直接加载到会计软件中，从而减少客户的管理负担。

#### d. 收银和转换服务

公司拟发展收银服务及转换服务。收银服务可以促使：

- 从银行账户中提取法定货币并将其转换成加密货币；和
- 将加密货币转换回法定货币并将其存入银行账户。



兑换服务将允许客户将代币转换为一系列其他加密货币。

通过提供收银和兑换服务，公司计划将ivyKoin网络作为一个端到端的解决方案，特别针对大额转账的企业。本公司将努力：

- 促进将法币兑换成加密货币；
- 促进加密货币在全球的转移；和
- 使收款人能够将加密货币兑换回在其银行账户中的法定货币。

最重要的是，根据预想，ivyKoin网络能够在不对发送或接收金融机构造成问题的情况下做到这一点。

#### e. 通过公开市场操作的固定价格转移

加密货币转移过程中潜在的货币损失是商家采用加密货币通常面临的最大障碍之一。公司的目标是开发一个固定价格的解决方案，消除由于加密货币价格波动造成的货币损失。

固定价格解决方案包括使用一个国库币池专门用于两个银行账户间的法定美元到法定美元的交易。通过ODFI（“原始存款金融机 构”）从发送人银行账户中提取法定货币。然后，ivyKoin网络将使用专门为此次目的而设计的场外货币库来将法定货币转换为代币（参见第7节）。

### 2) 金融机构

随着金融机构支持的增加，ivyKoin网络有可能用于以下交易，还有更多：

- 国内或国际货物采购；
- 企业对企业服务；
- 注定要成为金融机构中法定货币的一般价值转移；
- 软件许可证购买；
- 房地产购买；
- 全球投资；
- 大额个人转账；
- 小额个人转账。

### 3) 用户功能

根据建议，ivyKoin网络将提供一个对等方之间的价值交换，其中（1）发送方试图向接收方发送大量的加密电子货币，和（2）接收方收到该加密电子货币并使其成为银行账户中的法定货币余额。

发送人和接收人都可以使用代币将加密货币通过ivyKoin网络转移到金融机构，加密货币可以在ivyKoin.com和主要公开交易所购买。希望通过ivyKoin网络转移其他加密货币的账户持有人必须先将第三方加密货币转换成代币。

用户可以通过电话或移动设备访问ivyKoin.com，网站将为发送人提供以下核心功能：

- 账户开设和管理；
- 交易管理；和
- 代币购买、销售和转账



## a. 账户开设和管理

我们预计，发送人和接收人将能够在ivykoin.com上创建ivyKoin网络帐户，并在注册过程后收到独有的发送人身份信息。ivyKoin网络将保存所有发送人的帐户信息，以便他们不必为后续的转账提供相同信息。这个KYC信息由代表用户身份的各种数据字段和文件组成，例如姓名，电子邮件，电话，地址和政府身份。

完全开发后，帐户将能够通过 ivyKoin.com上的在线功能菜单进行管理，包括更新KYC和重复交易数据。账户持有人可以要求连接到其他ivyKoin网络账户持有人，并扩充已知和经过验证的加密货币付款对端名单，这在向相同接收人频繁发送或向新接收人快速高效发送时很有用。账户持有人可以在全球范围内的ivyKoin网络上让自己可见，并且一个账户持有人可以提出请求将其他账户持有人添加到他们自己的名单中。他们也可以使用ivyKoin网络服务转换代币并将其发送到自己在金融机构的法定货币账户。

### i. 发送人数据验证

ivyKoin网络意图是将验证基本发送人数据和银行账户的合法性作为开户流程的一部分。ivyKoin网络将使用各种第三方服务提供初始身份证件验证。身份证明文件，如护照和驾驶执照预计会在几分钟内完成验证。如果文件未被识别，则该账户将被置于待定状态以供进一步调查。同样，营业执照和其他注册公司文件也能够被迅速验证。

为了达到同样目的，我们打算使用一个程序来验证账户持有人的银行账户信息，在这个程序里小额存款会被存入账户持有人的银行账户，这些存款金额将被用于独立验证ivyKoin网络与银行之间的成功连接。

尽管做出了这些努力，但公司对付款的合法性或非法性不承担任何担保责任，尽管这种做法与现行网络非常相似。

## a. 交易管理

一旦ivyKoin网络帐户开立成功，我们预计发送人就能开始将代币转账给收件人。发送人将在交易之前将特定的交易信息输入到账户中。ivyKoin网络将要求为所有转移提供基础级别的信息，但根据适用的法律和法规不同可能会需要额外细节。ivyKoin网络将提示发送人提供与其交易相关的其他细节。例如，如果发送人正在进行付款以换取商品，则ivyKoin网络嵌入的转移信息可能包括产地，最终目的地，已支付进口关税证明或其他识别信息。发送人还可以选择提供有关转帐的其他详细信息 - 例如付款附带的发票副本。此外，如果发送人知道接收人不将其视为可信来源，则还可以添加质量保证证书，批量信息，公司章程以及其他广泛的自愿性KYT信息等信息。

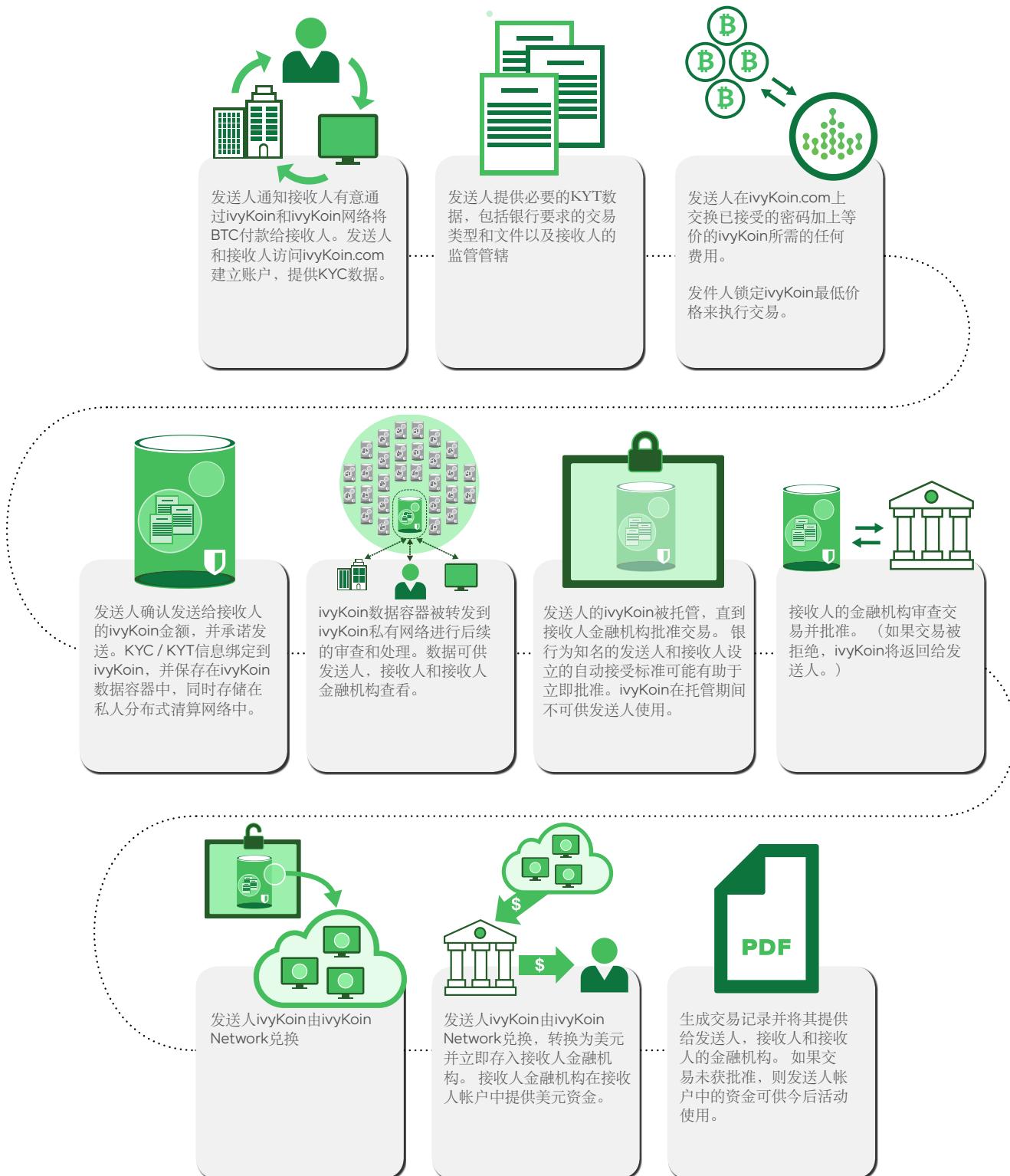
## b. ivyKoin的购买，销售和转账

我们预计，ivyKoin网络将促进资金和数据的安全传输，为发送人和金融机构带来共同的利益。当银行正在审查交易是否存在可以活动时，将拥有比传统支付网络和更现代的支付转账替代方案更庞大的数据点来协助审查。

付款价值将可以在区块链中公开查看，并且不能被删除。KYT和KYC数据将被加密并捆绑到由发送者发送给ivyKoin网络的代币，随后可由接收机构和接收人访问。此KYC / KYT / AML数据只能由交易相关方查看。

下面的图表从发送人，接收人和金融机构的角度描述了代币的预期流动。用户界面简单直观。

## ivyKoin转换为美元的功能流程图



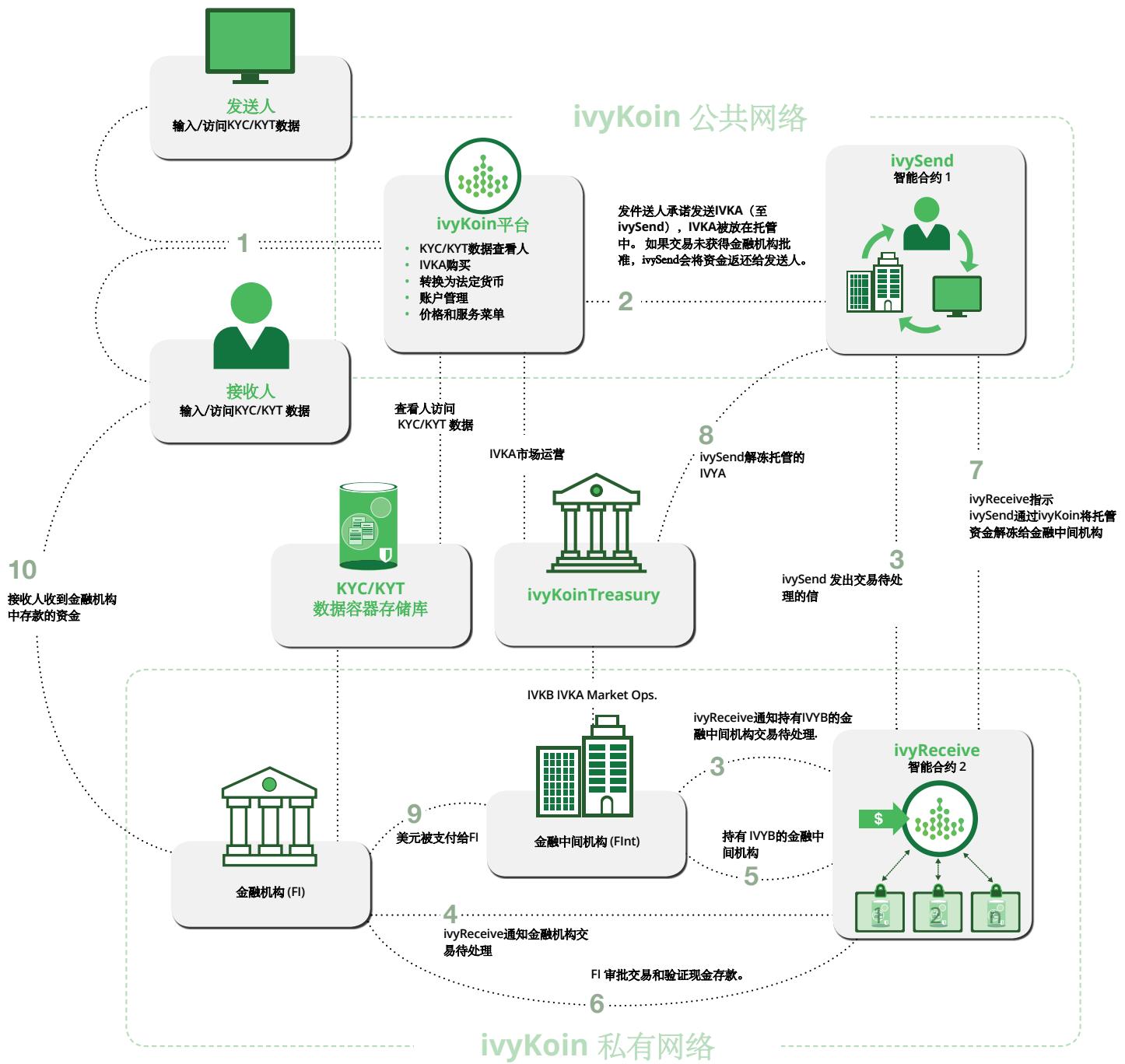
# 6

## ivyKoin技术规格

### 1) 技术架构概述

我们的意图是ivyKoin网络将通过使用双重网络架构来运行，其中代币的发送者在公共网络（**ivyKoin**公共网络）上操作，向法定货币提供财务结算的参与者在私人网络（**ivyKoin**私有网络）上操作。支持交易的KYC / KYT / AML数据将被捕获到由ivyKoin公共网络与ivyKoin网络智能合约交互产生的加密容器中，并且支持ivyKoin私有网络参与者实现交易结算的活动。这些数据将被储存并提供给金融机构和法定结余收款人的监管机构访问。以下技术规格在充分开发时预计将各自都成为ivyKoin网络的一部分。





### a. 公共网络, ivySend和公共ivYKoin代币(IVYA)

一旦ivYKoin网络投入使用, 预计寻求将第三方电子货币发送给预期接收人帐户的公共方必须在公开交易所中将其加密货币兑换成代币, 或直接从ivYKoin网络购买代币。 ivYKoin公共网络代币 (**IVYA**) 将被编写进以太坊网络上可用的ERC20规范。代币将被提交给以太坊上的ivYKoin网络合同 (**ivySend**合同), 并在那里被托管。托管状态在以下两个条件下被视为完成: a) 转账完成, 此时代币转移到ivYKoin网络, 在二级市场或公司网站上出售, 用于获取现金或第三方加密货币, 或者以其他形式燃烧; 或者b) 转帐失败, 在这种情况下, 向ivYKoin网络提交的全部代币都会被退还。

预计ivYSend合同将成为一个智能合约, 可以由任意数量的利益方从公共以太坊网络调用。在初步实施时, 很可能通过ivYKoin.com界面, 通过网站与以太坊网络的直接整合来提供。另外我们还设想, 其他各方同样会将此合同作为支付界面。ivYSend合同意图使用以太坊网络开采成本激励措施进行操作, 发送人必须承担合同的发起费用才能让合同在以太坊网络上进行处理。如果提交的开采成本不足以开采公共激励, 则托管合同将永不生效, 保证发送人的ivYKoin网络帐户余额, 从而可以继续交易的其余部分。ivYKoin网络费用也包含在ivYSend合同流程的成本中 (就像传统金融机构的电汇一样)。

我们预计, 寻求使用ivYKoin网络的一方可以使用公司的网站轻松查看a) 在各种常见的加密货币交易所中通用的加密货币到代币汇率; b) 成功执行ivYSend合同预计的以太坊开采成本收费; 以及c) 希望发送给预定接收人账户的给定法定货币余额的总代币费 (法定货币余额+开采成本费+佣金)。由于其中一些组成部分在总体定价中是不稳定的, 通过使用公司网站, ivYSend合同的用户可以在10分钟内收到执行报价, 报价会锁定含所报参数的给定ivYSend合同交易的执行报价在ivYKoin网络表示的在给出报价时的波动上限和下限内。

通过这种方式, IVYA在完全开发后, 将为其持有者提供全面的实用功能, 并保护其不受合同操作时波动的影响。

### b. 私有网络, ivyReceive, 和私有ivYKoin 代币(IVYB)

ivYKoin私人网络意图通过使用私人ivYNetwork合同 (**ivyReceive**合同) 将资金分配到预期收款人的银行账户。我们建议ivYKoin私有网络使用专用于金融机构和中间机构协调的以太坊区块链的私有链形式操作。

预计ivYReceive合同将托管在ivYKoin私有网络上。这将是参与金融机构和中间机构的结算账户通过使用私有代币 (**IVYB**) 参与风险的机制, 该私有代币将是一个与以太坊兼容的ERC20代币, 在ivYKoin私有网络上运行。ivYReceive合同的目的是规定ivYKoin网络如何使用IVYB直接结算收款人账户的余额。

在充分开发后, IVYB预计将成资产支持的代币, 反映了ivYKoin私有网络账户持有人拥有可以将交易清算到ivYKoin网络的法定货币储备金。IVYB将由本公司预先开采, 只能由公司转换为IVYA, 并按照其在ivYKoin网络中的储备比例交给ivYKoin网络账户持有人。至于公司对IVYB的使用方面, 公司意图对IVYB资产及负债进行公开会计处理, 以显示其在网络上的美元存款总是等于其托管和储备的代币持有量。

当待处理交易的信息到达ivYKoin私有网络时, 账户持有者必须以其IVYB押注, 以获得代表余额的机会; 这意味着ivYKoin私有网络账户持有人必须拥有至少等于交易金额的IVYB余额。在这种交互中, 押注代币的过程为向金融机构或中间机构发布KYC / KYT / AML信息提供了支持, 从中提示他们接受或拒绝资金 (手动, 或经预先授权自动)。这些代币被提交给ivYReceive合同。ivYReceive合同有两个强制放弃押注代币的条件:

a) 显示交易批准证明——在审查了适用的KYC / KYT / AML信息后, 适用金融机构的代理人会将批准或拒绝回复的信息发送给ivYReceive合同。在这种情况下, 有两个可能的结果:

交易成功完成, 在这种情况下, IVYB被退回, 并由ivYKoin私有网络账户持有人在金融机构内预定接收人账户中存入IVYB值; 或者, b) 交易失败, 在这种情况下, IVYB退还给金融机构; 和

- b) 显示现金存款——对ivyKoin私有网络账户持有人银行账户状态的监控提供了一种机制，通过该机制，金融机构显示对收款人账户的现金存款的已经发生。此状态可能需要为观察帐户状态进行定制集成，或使用来自供应商（如Yodlee<sup>13</sup>、Xignite<sup>14</sup>或Plaid<sup>15</sup>）的帐户访问服务进行类似操作。无论哪种方式，ivyKoin网络和金融机构之间的企业对企业的安排将规定帐户之间资金解冻的时间限制是什么。

如果“显示交易批准”和“显示现金存款”都显示为正确，那么在ivyKoin专用网络上押注IVYB的一方有资格从ivyKoin公共网络上解锁的ivySend合同中接收付款。如果两个条件都是错误的，或者在它们被设置为正确之前，ivyKoin公共网络上的ivySend合同可以由发送人来赎回。金融机构可能会拒绝批准交易，因为它试图通过使用与ivyKoin数据容器一起提交的KYC / KYT / AML数据来清理已识别的合规要求。使用与交易和容器相关联的元数据，有可能基于产地，商业中交换货物的性质或经手金融机构或中间机构所期望的其他可配置规则来实现一定程度的自动清算。同样，手动工作流程可能需要托管被额外保留一段时间。提交的默认行为是由发送人托管由ivyKoin私有网络上的结果决定；然而，可以设想的是，与银行KYC / KYT / AML过程带来的延迟以及发送者与接收者之间的通信也可能需要被适当考虑，由此在给定的延迟期之后，发送者可以通过选择将代币存款从托管中取出来结束这一过程。

我们的意图是让ivyReceive合同保持所有待处理的押注交易的可观察余额。ivyKoin私有网络上的许可提供了个人余额间的独立以及每个接收人金融机构和支持金融中间机构的待处理的结算工作流程状态。通过这种方式，被锁定在ivyReceive合同中的私有代币是为了：a) 提供对金融机构或中间机构考虑余额转移有效性的过程的可见性；b) 为金融机构的业务提供一个节流阀，这样如果没有将交易清算到满意的程度，他们就无法押注不成比例的交易金额。当然，这也提出了什么迫使金融机构或中间机构根据需要进行存款的问题。为此，ivyKoin网络将能够报告其网络中每个金融机构和中间机构的服务水平。显然，如果一家金融机构没有满足客户的需求，那么客户应该有能力从ivyKoin网络的其他参与者那里考虑其他的选择或机会，这些参与者在接收转账时要么更及时，要么更可靠。

#### c. 跨链通信和ivyKoin Oracle服务

ivyKoin网络旨在充当上述ivyKoin私有网络和ivyKoin公共网络之间的功能媒介，倾听和响应与ivySend合同和ivyReceive合同相关的事件。

我们预计，ivySend合约的状态变化会被参与公共以太坊网络的授权ivyKoin验证人观察到。同样，ivyKoin私有网络上的ivyKoin网络验证人也会观察到ivyReceive合同中的状态更改。这两个验证人组合都能够通知ivyKoin Oracle服务，该服务提供对每个托管合同状态的认证，并有助于实现它们各自的功能。

特别让人感兴趣的是价值如何从ivyKoin公共网络分类帐余额转移到ivyKoin私有网络分类账余额。这涉及从IVYA到IVYB的价值转移，在向ivyReceive合同发送批准消息和显示接收人银行账户到账余额时发生。在这两个事件发生的时候，IVYB被释放，而托管协议中的IVYA由IvyKoin网络要求解冻。IVYA通过使用ivyKoin Oracle服务及其中含有的对ivyKoin私有网络的验证工具收到ivyKoin私有网络分类账上对IVYB交易的确定。当IVYB被记入ivyReceive合同时，发送人给IVYB的公共地址将被记录。此公开地址用于将KYC / AML信息发送到ivyKoin交易容器。随后，此地址将用作ivyKoin网络的结算帐户地址，以私下结算其针对网络的交易。

---

13. <https://www.yodlee.com/>  
14. <https://www.xignite.com/>  
15. <https://www.plaid.com/>

## 2) 在ivyKoin网络上的身份

充分开发后，预计公司将管理ivyKoin网络上的两种身份：发送人身份，以及金融机构和中间机构身份。

### a. 发送人身份

ivyKoin 网络意图要求发件人在发送货币前在网络注册。ivyKoin网络认为，作为开设账户的一部分，接收人的身份应分别由金融机构和中间机构确定。

自主权身份就足够在ivyKoin网络上建立一个发送者账号；然而，想要获得ivyKoin网络授权可能需要额外的交易信息。此信息由发送人提交并存储在ivyKoin网络上以建立帐户，并允许公司为需要支持信息的特定交易类型提供证明。发送人自主权身份信息副本将打包在ivyKoin数据容器中，作为向预期余额接收方金融机构和其他中间机构提交交易一部分。虽然他们的用途有具体限制，这些凭证可能会被访问并且在交易之后一段延长时间内关联。使用公司的网站可以持续监控这些凭证的访问时间。

### b. 金融机构与中间机构身份

ivyKoin的意图是依赖在数据通信的金融机构和中间机构的良好雇佣实践和信息安全实践的警惕。想要公司跟踪所有雇佣事件，企业和人力资源相关活动在很大程度上是不切实际的。因此，ivyKoin网络将要求金融机构，中介机构和利益机构的相关合规人员的身份在ivyKoin网络注册，以启用和禁用对KYC / AML数据分布式容器的访问。金融中间机构的相关就业行为将在ivyKoin网络及时更新。

预计金融机构经理可以登录到ivyKoin网络来管理相关工作人员对ivyReceive合同职能和容器数据的访问和权限。所识别用户的所有活动都可以集中进行跟踪和管理，单个交易容器的历史记录也可以被查看。

## 3) 区块链技术应用

分布式账本的共识是验证人（有时也称为矿工）根据适当情况确定数据的准确表示以反映提交给网络的交易中正确分类帐余额的功能。考虑到网络和系统中断的可能，很容易预见到有些情况可能导致某些方断开连接，并在意外缺席时错过重要数据。

同样，在一个分享观点的网络中，需要建立一个确定的事实结果产生的成熟机制。在比特币和以太坊这样的网络中，目前的机制被称为“工作证明”。工作证明鼓励验证人根据计算能力和电力进行竞争，以验证提交给网络的交易。拥有更多计算能力有助于验证人解决更难的加密问题，这些问题随后提交给网络，以便抢先将捕获交易作为区块添加到网络中（顺便一提，这些交易区块是根据之前提交的其他区块的预测进行验证的，链条因此产生——因此术语称为“区块链”）。随着区块链的壮大，新区块的难度也随之增加——验证人为了验证激励和区块奖励的价值而花费巨大的代价进行竞争，他们希望在他们所在网络中捕获和重新分配这些奖励。在提供拜占庭容错的概念的同时，这个过程对于私有网络而言既昂贵又缓慢。因此，这就是比特币和以太坊每秒处理少于20笔交易的原因<sup>16</sup>。另外，由Tendermint实施并提出的共识机制“权益证明”是对以太坊的Casper共识的改进，将获得添加分类账交易区块的权利的费用从计算和电力投资转向了对加密货币本身的投资<sup>17</sup>。在权益证明中，拥有更多加密货币比例的一方在添加下一个交易区块上也有更多比例的可能。由于每个验证任都在网络中“押注”，网络可能由于他们的恶意行为收回他们在网络中的权益来对他们进行惩罚，这些恶意行为会导致产生虚假交易区块的产生，这就需要网络的其余部分进行后续校正。然而，这种方法会带来挑战主要有两个原因：a) 任何一方或拥有51%网络价值的串谋方更有可能获得共识；和b) 通过计算能力的投资，恶意的大多数不能被推翻，因为工作证明是允许的。此外，正如工作证明需要验证激励措施来使验证者以区块奖励的形式捕获交易，权益证明同样使用激励措施（例如“开采成本”）来防止只为网络创造工作而没有相应财务价值的交易的提交（例如：垃圾信息）<sup>18</sup>

16. <http://www.altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/>

17. CIT

在金融支付网络中，特别是私人和被许可的网络相比公共匿名网络更容易通过利益分享而被组织和管理，因此调整激励措施以防止可疑行为的问题会导致对实际吞吐量和能够促进准确和合规结算的协调功能的灵活性的担忧。包括Stellar和Ripple在内的网络使用他们自己的验证人，或者验证人的共同参与来屏蔽他们对网络结果的直接输入<sup>19</sup>，因此就不太可能出现外部和恶意参与者。在这里，他们的共识是通过他们的网络关注分布式账本的灵活性和可用性。结果是吞吐量更高<sup>20</sup>。

公司设想，ivyKoin私有网络将由除本身之外的实体赞助的验证节点组成。ivyKoin私有网络将直接由独立但有序的金融机构和中间机构进行验证。在这种环境下，来自被许可的网络参与者的垃圾信息几乎不太可能，甚至首先就对他们参与ivyKoin网络的共同目标有害。网络垃圾可能性大大降低和激励机制的调整，消除了通常用于激励公共区块链网络的区块奖励的需要。至于共识，使用计划的拜占庭容错算法（如伊斯坦堡BFT）是最有意义的。<sup>21</sup>在这种共识算法中，每个参与者都以预定的轮询调度方式创建区块，并将其结果提交给网络的其余部分，必须有2/3的多数表决才能批准领导者的区块计算。这种方法可以在网络中大约1/3的验证人可能被证明是恶意的同时仍然证明网络的灵活性。伊斯坦堡BFT的具体基准表明其能够每秒处理约1000次交易，<sup>22</sup>这反映了今天在FedWire、SWIFT和ACH之间发生的跨部门交易网络的总和。<sup>23</sup>

就其目的而言，我们预计，ivyKoin私有网络最初将采用Quorum，JP摩根大通实施的使用伊斯坦堡BFT共识算法的经许可的以太坊。<sup>24</sup>以太坊的实施对于ivyKoin网络有许多潜在的好处：a) 它提供了在全球金融机构范围内验证和改进的以太坊区块链好处；b) 它提供了与智能合约开发和投资的互操作性，可以将其原型化，并可以移植到任何其他以太坊虚拟机（EVM）支持环境（包括Ethermint，Qtum，甚至是公共以太坊区块链）；<sup>25,26</sup>和c) 因为是被人熟知的金融界另类区块链，其采用和使用提供了社区和支持的基线，最有可能获得公司寻求支持其网络功能的同样的金融机构和中间机构的支持。Quorum还支持基于主要验证人授权的替代共识算法，如果需要更高的交易吞吐量，网络参与者的意图的稳定性能够减少区块验证开销。

- 
- 18. 在公共场所，潜在的垃圾信息交易可能涌入合法交易，造成类似于拒绝服务攻击中存在的环境；如果验证人正在为无价值交易消耗精力，那么有价值的交易处理起来就会更难。
  - 19. CIT - 恒星分片
  - 20. CIT
  - 21. 拜占庭容错或（BFT）是计算机科学中解决分布式系统网络内协调问题的一个问题参考，通常称为拜占庭将军问题，在这个问题中，任何留在自己的设备上的单个系统参与者都被激励为自己的利益而工作，而不是网络的真实利益。
  - 22. <https://www.slideshare.net/YuTeLin1/istanbul-bft>
  - 23. CIT
  - 24. <https://github.com/jpmorganchase/quorum>
  - 25. CIT [Ethermint 白皮书]
  - 26. CIT [Qtum 白皮书]



私有网络节点使用IPFS和BigchainDB进一步协调数据交换，以确保可用性和数据完整性。<sup>27</sup><sup>28</sup>私有网络节点的逻辑表示如下图所示：



ivyKoin 私有网络节点概念图

#### 4) ivyKoin 数据容器

预计ivyKoin网络将使用dxChain加密容器将KYT / KYC / AML数据存储在日期容器（ivyKoin数据容器）中。数据在用户提交货币转账请求时通过ivyKoin应用界面被收集。ivyKoin数据容器的这种特定容器格式如下图所示：



ivyKoin 数据容器

ivyKoin数据容器的内容意图涵盖：

- 容器元数据
- 交易元数据
- 提交的交易明细
- 发送人身份信息（如适用）
- 支持性文件和附件

使用这种格式，支持数据的每个组成部分都是独立和持久加密的，以便在使用标准AES-256对称加密和4096位RSA非对称加密方法以及SHA-384消息摘要进行交换期间能够安全访问。预计基于RSA非对称密钥的数字签名易受Grover<sup>29</sup>和Schor30算法对应用量

27. <https://ipfs.io>

28. <https://www.bigchaindb.com>

29. [https://en.wikipedia.org/wiki/Grover%27s\\_algorithm](https://en.wikipedia.org/wiki/Grover%27s_algorithm)

子计算来确定黑盒函数输入和大数分解上的影响，在行业有更好的理解并能提供更好支持的情况下，这些算法将分别升级以反映量子抵抗算法的可用性。<sup>31</sup>

加密容器意图为ivyKoin网络提供几个关键特性：

- 提供持续控制和保护所有沟通信息；
- 让ivyKoin网络能够在首次接收之后将各方添加到容器中或从容器中移除；和
- 为发送人提供保证，其与接收人交易的具体内容是保密的。

通过使用ivyKoin数据容器，可以跟踪和验证针对网络的个人行为。

ivyKoin数据容器意图存储从ivySend合同提交过程中收集的结构化和非结构化内容。在适用的情况下，ivyKoin会将ivyKoin数据容器内的数据收集标准化，以符合ISO 20022标准的数据集，代码和格式。<sup>32</sup>

#### a. ivyKoin数据容器的生成和存储

充分开发后，向ivyKoin网络合同提交内容时，会向ivyKoin网络发出请求以生成相关数据的容器。这项应用会将提交的KYT / KYC / AML数据发送到ivyKoin网络，并将容器标志符返回给发送人。发送人将他们的ivyKoin存款和生成的容器标志符提交给ivySend网络合同。

生成后，ivyKoin数据容器将被保留在托管于ivyKoin私有网络范围内的IPFS文件系统上。ivyKoin私有网络文件系统将允许共享网络中的相关内容。<sup>33</sup>为确保文件有余，容器对ivyKoin私有网络会有三个独立写入，因为在请求时只能保证提供本地副本。这些容器标志符和ivyKoin私有网络上的对象标志点的映射存储在ivyKoin私有网络节点之间共享的BigchainDB网络中。<sup>34</sup>

检索ivyKoin数据容器包括通过生成容器的容器标志符来查询BigchainDB网络，以接收用于检索相关容器的相关对象标志符。在ivyKoin网络中，该功能由被许可的网络上的托管服务被抽象化和维护。ivyKoin数据容器可以自由复制和存储，而不会违反其基础安全模型。

#### b. 访问ivyKoin 数据容器

我们的意图是让访问ivyKoin数据容器由网络绑定的访问管理服务管理，该服务负责处理对ivyKoin数据容器内容特定部分的请求，并根据以下标准提供必要的访问权限（用于简化，用户，系统和系统进程的目的被视为用户请求）

- 请求得用户组织——确定KYC数据是否与请求用户组织发生的交易相关，或者，如果请求用户组织是监管机构；
- 请求用户提交的凭证——确定请求用户的凭证是否为ivyKoin私有网络帐户持有者与ivyKoin身份管理环境之间的每次通信的当前信息；和
- 对请求用户提交的凭证和请求的特定身份信息类型的具体管理限制。例如，标识为个人信息特定信息可能不能提供给所有请求的用户。这些限制由成员金融机构的管理人员和ivyKoin网络进行协调。

成功授权给ivyKoin数据容器后，请求的内容将呈现给请求的用户或进程。

---

30. [https://en.wikipedia.org/wiki/Shor's\\_algorithm](https://en.wikipedia.org/wiki/Shor's_algorithm)  
31. <http://nvlpubs.nist.gov/nistpubs/ir/2016/NISTIR.8105.pdf>  
32. <https://www.iso20022.org/>  
33. <https://ipfs.io/>  
34. <https://www.bigchaindb.com>

# 7

## 代币生成事件后代币结构

ivyKoin在计划的代币生成事件(TGE)前正在进行ivyKoin代币的预售。

### 关键信息

预售开始	2018年1月16日
保证分配期 <sup>1</sup>	2018年1月29日
预售结束 <sup>2</sup>	2018年2月9日
预售代币发售	1.5亿 <sup>3</sup>
预售代币价格	0.10美元
预售筹集金额	1,500万美元 <sup>3</sup>
代币生成事件 <sup>3</sup>	预计在2018年第一季度
代币总发行量	约15亿
流通供应市场资本	8,400万美元 <sup>4</sup>

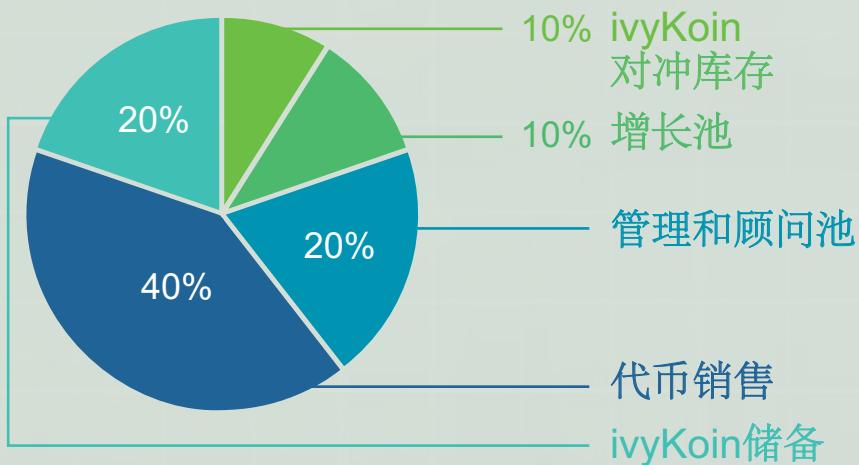
\*不包括交易所上市费和开价成本

- 
- 面向总经理接受投标的合格投资者。
  - ivyKoin保留提早关闭预售或酌情延长的绝对自主权。
  - ivyKoin保留全权决定更改筹集金额的权利，最高总额为15亿ivyKoin供应量。这个数字只是一个估计，公司并不保证这个数字会实现。
  - 该数字只是一个估计值，公司并不保证这个数字可以实现。基于TGE的1500万美元的筹集和流通供应。非流通供应包括为建立全球财务伙伴关系，机构合作关系，法定对冲和未来代币销售而保留的代币。

## 收益使用<sup>5</sup>



## 发行后持有情况 – 代币总量



## 图释

- 代币销售——包括所有出售给TGE的代币，包括所有之前的代币销售和相关的代币费用。
- ivyKoin储备——仅用于在需要时为进一步的开发和运营成本提供资金。
- 增长池——用于激励包括金融机构在内的合作伙伴来测试和采用ivyKoin.
- ivyKoin库——用于促进ivySend交易和其他财务功能。
- 管理和顾问池——激励现任顾问和未来管理层加入公司.

5. 此饼状图仅为估计，公司保留在认为合适的情况下全权决定如何使用任何和全部收益的权利。

# 8

## 路线图

以下日期和时间分别出于预测和展望。

### 近期

#### H1 2018:

- 代币生成事件(Q1 2018)
- IVYA公开可用
- 测试网络上线配合智能合约
- KYC/KYT交易容器
- ivyKoin 公共界面上线
- 与金融机构建立合作关系
- 与美国监管机构谈判

#### H2 2018:

- 公共网络上线
- ivySend上线配合传统跨行系统
- ivyKoin指导IVYA销售和市场运营上线
- ivyReceive上线配合IVYB跨行资金转账
- 加速金融机构合作关系

#### a. 代币

私募配售完成后，公司意图在可行情况下尽快进行代币生成事件。想要了解更多信息，请参阅公司提供的代币生成事件的条款和条件。

#### b. 操作

代币发行有两个部分：

- **代币生成事件：** 初始代币将被铸造以太坊代币
- **全面流通和转换：** 功能完善的代币在以太坊上可用。

## 中期至远期

2019

- 所有法定货币/加密货币转换上线
- 企业授权给容器
- 第一批金融中间机构



我们意图将ivyKoin网络开发在在2018年分两个阶段进行。在ivyKoin网络开发的第一阶段，通过传统的跨行支付方式（如ACH或电汇）直接从公司收到付款。在第二阶段，银行从ivyKoin网络验证人那里收到付款，这些验证人在网络上进行私人IVYB转账，并通过他们在那里维持的账户直接付款给成员金融机构。随着时间的推移，公司将努力：

- 在全球建立参与的金融机构网络
- 扩展转换功能，囊括更多法定货币和数字资产
- 与可以从ivyKoin网络受益的组织建立伙伴关系
- 开发用于KYT / KYC / AML数据验证的改进方法

# 9

## 风险

权利和代币被认为是高度投机的，购买权利和代币带有一些风险。董事强烈建议潜在买家考虑下文所述的风险因素及本文其他部分所载的资料，并在决定是否购买权利和代币之前咨询其专业顾问。

如果潜在购买者不能接受以下任何风险，则潜在购买者不应购买权利或代币。

以下列出的风险顺序无意影响发生此类风险的可能性，或任何此类风险对任何特定购买者的重要性。

只有对比特币和以太币以及其他基于区块链的软件系统等加密货币的使用和复杂性有着丰富经验和理解的个人或实体才能购买权利和代币。购买者应该对与其他加密货币相关的存储和传输机制有切实的理解。

公司不提供任何建议，公司也不对由于购买者采取或不采取行动而导致的任何资金损失，权利或代币损失负责。

### 失去访问权限

代币可以存储在钱包中，并且可以通过密钥签名（和其他方式）访问。与购买者的数字钱包相关联的必要私钥丢失将导致存储的代币丢失。如果购买者没有保存其私钥或用于访问其私钥的密码的准确记录，则可能导致永久性失去对其代币的访问权限。购买者必须将其密码安全地存储在与主要位置完全分离的一个或多个备份位置中。任何获得购买者私钥的第三方都可以访问购买者的代币。如果潜在购买者没有这样的经验或专业知识，则不应该购买权利或代币。

### 与加密货币协议相关的风险

代币的基础是加密货币协议。ivyKoin协议的任何故障，意外功能，分叉，故障或废弃都可能对代币产生重大不利影响。例如，这可能对购买者转移或安全持有代币的能力产生不利影响。此外，密码学或量子计算发展的进步可能导致支持ivyKoin协议的密码共识机制失效。任何此类影响都可能对代币的价值产生不利影响。



## 开采攻击

在验证IvyKoin区块链上的代币交易的过程中，代币很容易受到矿工的攻击，包括但不限于重复消费攻击，多数开采力量攻击，自私开采攻击和竞赛状态攻击。

任何成功的攻击都会给代币带来风险，包括但不限于准确执行，记录涉及代币的交易以及预期的适当支付操作。

## 黑客攻击，网络威胁和安全弱点

黑客，个人，其他恶意团体或组织可能试图以各种方式干扰代币及其交易平台，他们在平台上的行为多种多样，包括但不限于恶意软件攻击，拒绝服务攻击，基于共识的攻击，Sybil攻击，“蚂蚁搬家”和幌骗交易。

代码破解的进步或量子计算机发展等技术进步可能会给代币带来风险，这可能会导致代币被盗或丢失。

## 市场风险

公司不能完全控制任何或全部代币购买者的行为。即使第三方交易所能够实现代币的二级交易，这种交易可能相对较新，并且很少受到或不受监管监督，因此更容易受到欺诈或操纵。此外，如果第三方确实认为外部交换价值属于代币（例如以法定货币计价），则此价值可能非常不稳定并且会减少至零。如果购买者选择在交易所使用代币，风险由购买者自行承担。此类交易所独立于公司，不受公司运营或控制。

## 交易所风险

发生代币交易的加密货币交易所可能相对较新，并且很可能基本不受监管，因此可能比完善的受监管的交易所更容易发生欺诈和故障。在代表大量代币交易的加密货币交易所涉及欺诈或经历安全故障或其他操作问题时，这种加密货币交易所的故障可能导致代币的价格和价值降低。

## 没有保险和交易损失

与在银行或一些其他金融机构的账户中持有的资金不同，除非购买者专门获得个人保险，否则代币一般不会获得保险。在代币丢失或使用代币的能力丧失的情况下，没有关于代币的公共保险公司或私人保险。

如果代币被盗或者被错误转移，这些代币可能无法收回，对此公司不承担任何责任。因此，任何不正确执行的代币交易可能会对代币的价值产生不利影响。

未经交易接收人的同意和积极参与，或者理论上，若无主机区块链平台上的大多数处理能力的控制或共识，加密的代币交易是不可逆的。一旦交易已经被验证并记录在被添加到区块链的数据块中，代币的错误转移或代币的被盗一般是不可逆的，并且可能没有针对该转移或被盗的法律途径或其他追索或补偿。这种损失通常会对代币的价值产生不利影响。

## 不确定的法规，执法行动和地缘政治事件

加密代币，区块链和分布式账本技术的监管状况在许多司法管辖区尚不明确或尚未确定。很难预测监管机构如何或是否可以将现有法规应用于这些技术及其应用，包括代币。同样很难预测的是，立法机构或监管机构如何或是否可以对影响区块链和分布式账本技术及其应用（包括代币）的法律法规进行更改。

监管措施可能会以各种方式对代币产生负面影响，包括仅为了说明目的，通过确定代币是一个或多个司法管辖区中受监管的金融产品或工具，诱导对其施加披露，注册或许可要求，或者干脆禁止使用代币或涉及代币的交易。

如果监管行为或法律法规的变化导致在此类司法管辖区内运营非法，或在商业上不希望获得必要的监管批准或为了在该类司法管辖区运营而满足相关监管要求，公司可能会终止在某一司法管辖区的运营。



政治或经济危机可能会刺激代币的大规模销售，这可能导致价格下降并对代币的价值产生不利影响。像代币这样的加密代币受供给和需求力的影响，这基于另一种去中心化的交易手段的可取性，而且这种供求如何将会如何受到地缘政治事件的影响尚不清楚。代币的大规模销售会导致此类代币的流动性下降。

## 税

权利和代币的税收特征以及持有权利和代币的税收后果在许多司法管辖区尚不确定。购买者必须就购买权利和代币寻求自己的税务建议，这可能会对购买者造成不利的税务后果，包括但不限于预扣税，所得税和税务申报要求。购买者对购买，使用和持有代币的任何税收要求承担全部责任。

## 不利的货币波动

公司意图将销售权利所得收益用于代币的维护及开发。发售的收益将以美元计值。如果在发售期间或之后美元价值波动不利，公司可能无法资助代币的开发。

## 极端波动

我们的意图是不让代币代表任何正式或具有法律约束力的投资，并且一旦开发就不需要在任何公共市场上进行交易。此外，在公共市场上具有价值的加密代币经常在短时间内出现极大的价格波动。这种波动是由市场力量造成的，代表了供求平衡的变化。交易所和公共场独立于公司并且不由公司运营。任何交易所或公开市场上的交易风险均由每位购买者自行承担，公司不能保证代币的任何市场流通性或可销售性。

此外，不同司法管辖区的不同监管要求以及某些司法管辖区公民可能无法在全球各地的交易所开立账户，因此代币在不同司法管辖区的流动性可能会有重大差异。这可能会反映在市场之间巨大的价格差异上。代币的价值也有可能在未来大幅度下降。代币价值的任何这种下降都可能对公司筹集持续经营资金的能力产生不利影响，包括代币的开发。

竞争的加密货币相比代币对重要的加密代币用户群来说更为理想，或者由于技术的整体信心的下降，加密代币的使用可能会普遍下降。任何此类事件都可能导致代币的需求和使用减少，这通常会对代币的价格产生负面影响。

此外，由于欺诈，企业倒闭，黑客或恶意软件或政府规定的监管，加密货币交易所缺乏稳定性以及加密货币交易所倒闭或暂时关闭都可能导致代币价格有更大波动。

## 知识产权索赔

第三方可以提出与权利或代币相关的知识产权所有权和/或其源代码或其他相关知识产权的索赔。不管任何知识产权索赔或其他法律行动有何好处，任何威胁的行为都可能会对代币的价值产生不利影响。

## 无法预料的风险

权利和任何待开发的代币都代表了一种新的相对未经测试的技术。

除上述风险外，还存在与购买权利或代币，持有权利和代币以及使用权利和代币相关的其他风险，包括公司无法预料的风险。

无法预料的风险可能以上述或其他方式风险的变化或组合形式出现。

# 词汇

## 以太坊

以太坊是一个领先的智能合约去中心化平台，采用Solidity编程语言。它是一个开源的基于公共区块链的分布式计算平台。

## 以太币

以太坊区块链平台的价值代币被称为“以太币”。

## 智能合约

智能合约是编程的抽象思想，明确表示各方之间交换关系的确切条款。在交易被记录和执行之前，智能合约条款必须被满足并被确认为“真”。智能合约是用Solidity这种编程语言编写的。所有这些智能合约都公开存储在每个区块链节点上。

## IPFS

是一个开源的、去中心化的文件系统协议，为文档的创建，存储和共享提供了永久的方法。IPFS节点构成了分布式文件共享网络的基础。这是一个基于块存储模型的高吞吐量。它利用散列进行文件识别，为不可改变的数据存储创建强大的环境。

## SOLIDITY

区块链的智能合约是用称为Solidity的编程语言编写的。

## X509

公钥证书定义的密码标准。它是安全通信的关键组件，可用于验证电子交易中的“数字签名”。X.509由国际电信联盟（ITU）定义，该电信联盟是负责全球电信和标准协调工作的联合国机构。

## PKI

公钥基础设施（PKI）是创建，管理，分发，使用，存储和撤销数字证书所需的一组角色，策略和过程，也是基于公钥的加密系统的关键组成部分。

## 信任链

信任链是通过自下而上验证硬件和软件的每个组件来建立的。这可确保通过验证链中的每个硬件和软件组件，只有可信的软件和硬件才能使用。

## 数据域

交易中发送的数据量根据各方的要求以及管理交易的智能合约的要求而异。ivyKoin不会验证客户数据（超出简单的账户开设过程范围）而是促进这一过程。



**ivyKoin**

**Ivy Koin LLC  
Ivy Management Group LLC**

**468 N. Camden Drive, Suite 200,  
Beverly Hills, CA 90210**

**[www.ivyKoin.com](http://www.ivyKoin.com)**