The Credit Protocol Whitepaper v1.0.1

Blockmason Team

2017-08-15

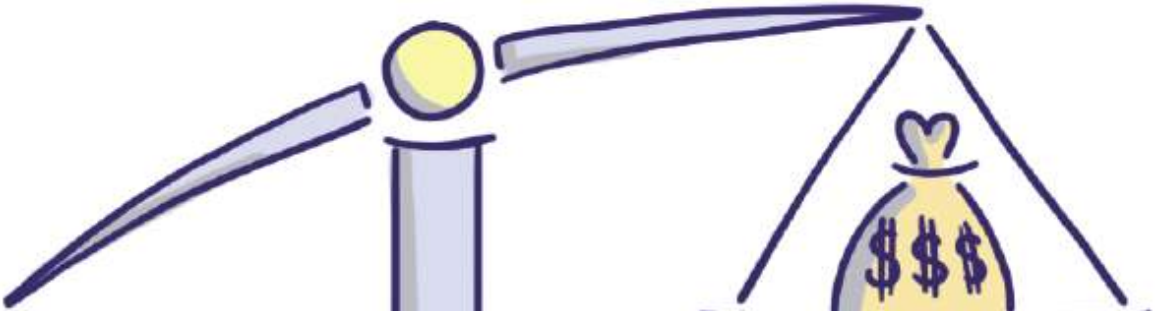
简介及其特性：

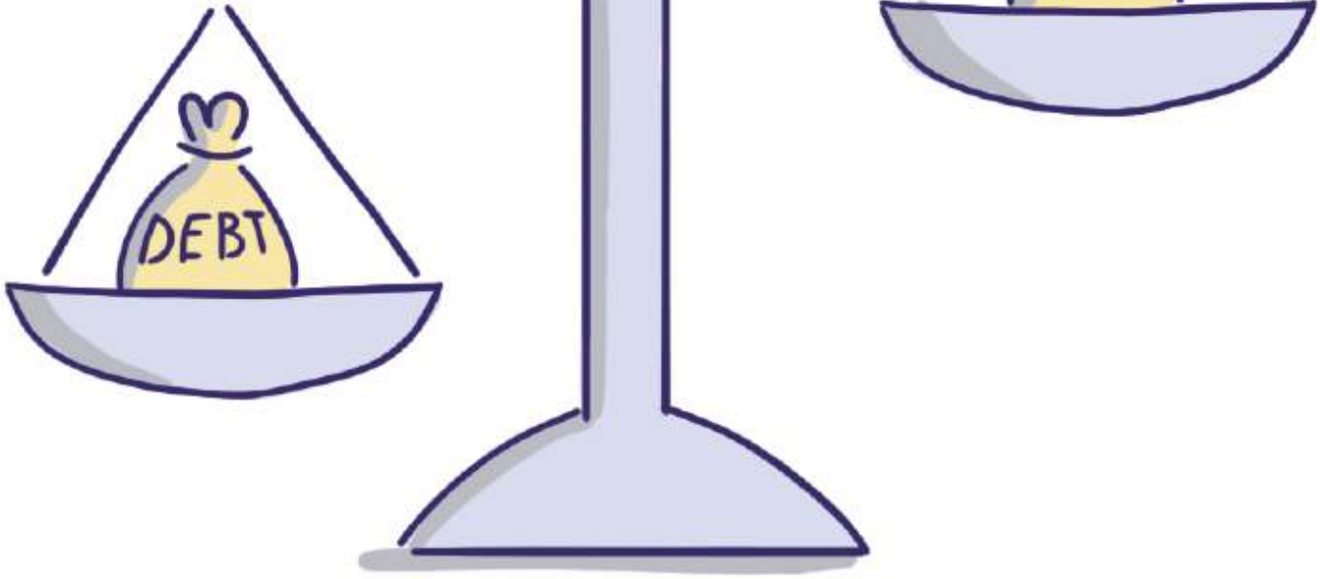
我们可以透过3种方式来思考以以太坊(Ethereum)为基础的全新协定：其为用户创造的价值、其为开发者创造的价值、以及其为社群创造的价值。在BlockMason，我们不仅致力于建构实用的应用程序(application, App)和协议以解决现实社会的各种问题，更致力于开发各个平台以扩大以太坊网络的采用率及加密货币(cryptocurrency)在全球范围内的可近用性(accessibility)。

这也是为什么我们会如此兴奋地向各位宣布我们最新开发的产品：**信用协定 (Credit Protocol, CP)**。

截至目前为止，我们只能以现金的形式将钱存放在区块链(Blockchain)上。比特币促成金钱在移转和储存方面的自主化(democratize)，以太坊则令建立和储存金融合约的过程更自主化。在信用协定(Credit Protocol, CP)下，BlockMason已在去中心化(decentralized)的经济体系中踏出具逻辑性的重要一步：*使信贷产生的过程更加自主化*。债务(Debt)和信贷(Credit) 本来已是极为强大的金融工具，而如今，利用区块链具安全性且灵活特质，可以广泛增加这传统金融工具的应用。运作方面，即使用户毋须拥有以太网络，亦可以轻易从以太网络中提取债务，因此我们可以完全想象在不远的未来，CP的债务应用市场总值将会远超越所有加密货币的市场总值，从而显著地提升数字经济(digital economy)的规模。

我们可以完全想象在不远的未来，CP的债务应用市场总值将会远超越所有加密货币的市场总值，从而显著地提升数字经济(digital economy)的规模。





我们开发的产品能充份反映团队的视野和最佳的执行能力。在BlockMason，我们并未着眼于空洞的承诺或亮眼的白皮书。没错，令我们感到自豪的是，我们的团队完成了本文件的制作；但更令我们自豪的是我们的开发者。开发者针对我们最新的应用程序—友人债务(FiD)—完成了一项功能完善的beta 测试版本部署，以展现CP的功能性。此一简单好用的分布式应用(DApp)目前正对外发布进行测试。尽管来吧! 您也可以登录 fiddy.io，并下载有关应用。我们非常期待您的试用...

噢! 您终于回来了。好吧，在您深入了解全新的CP以前，我们还有一件事情要和您分享：

在您购买首次货币公开发售(Initital Coin Offering, ICO)的产品专用代币(token)时，您不仅要注意产品是否按原样出售，更要考虑该公司为顾客提供产品支持的能力。这也是为什么我们将在ICO前后持续更新和改善CP。和其他ICO不同，我们的产品一枝独秀，符合各方期待且相当具有潜力，并能在我们扩展区块链技术的可能性时展现本公司对持续开发、产品维护和创意的诸多承诺。我们并非因有资金来源才对产品投入热忱及改善以太坊生态系统(ecosystem)。我们的目标是要证明我们热衷于建构有用、实用又能改变生活的DApp。

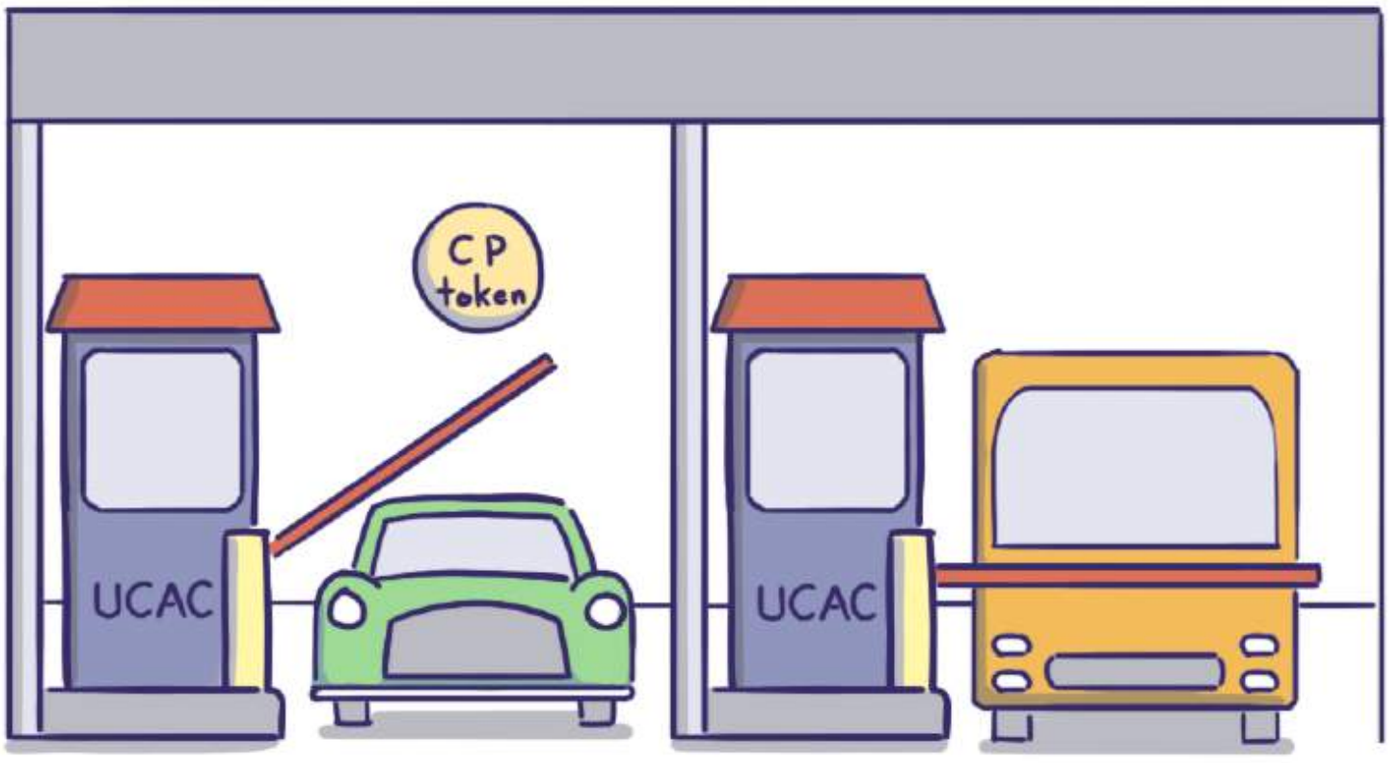
信用协定 (Credit Protocol, CP)

在其最为基础的层面上，CP是一个可将实体之间的债务和信贷记录在以太坊区块链上的系统。当甲方实体向乙方实体传送一项债务或信贷请求，乙方实体确认有关债务或信贷后，该交易纪录便会储存在CP的智能合约(smart contract)上。

实体之间透过CP进行简单的互动，若与一个根据有关协议加以建构的使用案例权限合约(Use Case Authority Contracts, UCAC)相互结合，就能创造一个强大而复杂的潜在交易数组(array of possible transactions)。每一个UCAC都有独特的规则来规范可被记录的债务类型、记录有关债务的时间、以及可被接受的提取者。例如，一个UCAC可能只允许某些通过认证的用户进行交易，从而让有关机构得以建构私人债务记录合约。有关合约的用途很广，从追踪应收帐款到开发私人组织货币(如大学校园都在使用的校园币)，应有尽有。

在许多方面，这套系统就类似一条高速公路。每一个债务或信贷就像一台车辆—其款式、型号、特性和色调各不相同，但他们基本上都有一个类似的用途。在一台车辆上高速公路后，此项债务及其相关特性，都会被记录下来。当然，您可能希望有某些规范能确保交通顺畅以及相关车辆能顺利抵达正确的目的地。开发者可在高速公路入口建构其独特的收费站或UCAC。每个收费站都能完全控管能驶入公路上的车种、能行驶的特定路段、以及于什么时段能在公路上行驶。然而，营运一个收费站亦需投入各项资源，CP的用

户可购买CP代币(CP Token, CPT)去支持收费站和公路的营运，同时，用户也保有是否把营运费用转嫁给行驶过的车辆(债务/信贷)或允许其免费通过。



The CP

影响收费站的车辆流量有2项因素：有多少个CP代币用于资助收费站的运作，以及每一个CP代币可进行的交易次数。基于网络车流量，CP代币可进行的交易次数都会有所不同，换言之，每一次的交易成本都会因应网络需求量而调整。

而UCAC就是透过CP代币去购买债务记录的容量。简单而言，使用CP的授权，跟软件使用者付款后能取得软件的授权使用之概念极为相似。唯此CP代币拥有者可以取得永久授权使用，所以用户可以在能够保留CP代币和权利下，选择把授权使用交易转让（sublease)给其他有需要的用户。

使用案例权限合约 (Use Case Authority Contracts, UCAC)

UCAC可视为输入和结算债务的一种途径。由于UCAC是由用户创造的，因此，系统用户或机构能够根据需要去制订记录债务的具体合约细则。可以编写在UCAC的内容包括货币类型、大小和允许交易的频率(用户可以从此建立债务，扩大信贷额和限制所累积的债务)。只要债务交易能与CP兼容，细则订立者能不

受限制地根据需要去创造有效、有价值的UCAC (唯一的限制将是细则订立者的想象能力) 。

每一个UCAC都要求操作者"**投注** (Stake) "至少一个CP代币，方可透过UCAC将债务或信贷写入CP系统。每一个CP代币允许UCAC每天处理一定次数的交易，而CP代币每天的交易次数会根据流量不断更新。因此，投注更多的CP代币就能提升和确保UCAC每天的交易量(throughput)。根据用户或开发者对债务系统的选择，他们可能须持有多个CP代币才能维持UCAC理想的交易量。一个CP代币可以被分拆成较小的代币单位，但如果用户拥有的CP代币单位太小，该用户所持有的CP代币可能无法用来产生交易。另外，一个CP代币产生出来的被允许交易次数将在交易产生后的24小时后失效。此时，CP代币亦将产生一组新的可用交易。

UCAC的悬赏计划 (Bounty Program for UCACs)

我们已花费大量的篇幅来解说UCAC和CP的关系。现在我们也知道，CP必需有与UCAC共同使用，才可以产生广泛的应用。由于编写在UCAC的内容可以产生无限的变化，且创造有关合约的需求各异，因此CP于ICO后将搁置CP代币部分的销售收益，以便资助和激励开发者去编写各类型高需求的UCAC。

免费存放UCAC (Free UCAC Depository)

在BlockMason，我们致力为CP及其用户提供绝佳的顾客支持。达成此一目标的关键在于，建构一个对CP有信心的支持社群，并进一步开发其独特的生态系统。因此，我们将为开发者创造和保留一个可免费存放UCAC的存放处(depository)，以便开发者以后根据CP再建构其他的DApp。此存放处将包括悬赏计划的所有得奖者，以及能后期加以客制化定制的UCAC的模板(template)。此一存放处不仅可促进CP社群的增长，更可让有兴趣人士浏览UCAC在世界各地的成功应用案例，以推广用CP的广泛支持。

Foundation ID

7月1日，BlockMason已免费对外发布全新的Foundation协定(Foundation Protocol)。[1] 我们开发Foundation的目的是希望能够将多个电子货币包(wallet)整合统一的问题。我们相信Foundation能解决应用开发者遇到的阻碍。而且我们相信Foundation与CP的融合会是取得成功的关键。

Foundation ID可以从多个以太坊地址创造单一一个主要ID (Master ID)，以便在以太坊网络上为用户建立一个统一的身分识别和交易平台。持有Foundation ID的用户可在无须来回传递私人密钥的情况下，轻易地同时登入多个DApp (类似案例：多数的网络应用程序都能透过Facebook或Google账户进行登入)。CP的所有用户都能于初期，免费使用Foundation ID，钱包整合统一化将改善用户体验并降低使用有关应用程序的进入门坎。

请参看以下篇章： Foundation Technical，以了解更多信息。

强制执行债务偿还 (Enforcing Debt Repayment)

尽管CP可为记录债务和信贷提供多项功能，但值得注意的是，个别用户仍须就如何偿还债务的执行方式取得共识。此执行方式可以多种方式进行，并可涉及到区块链上和区块链外的方案，其中包括：具有拘束力的法律合约、可为实体/数字资产的抵押品，或区块链上的信贷报告或交易评价等社会机制。

当然，用户不应把钱借给偿还债务能力有问题的实体。用户亦不应出借自己可负担范围外的金额。

然而，透过灵活制订UCAC和设置，我们确有可能制定完全符合个别用户和企业需求的债务合约，然却也会因此产生债务执行的问题。我们已于下方为CP介绍使用案例，并提出2个常见的债务情境如下所示：

1. Jesse欠其朋友(Tim)一罐啤酒。
2. Jesse的公司(Jesse Corp.)为其顾客Tim发送一张礼券。

在情境1中，若其债务透过UCAC被记录在CP上，社会压力足以令其偿还债务—如果Jesse不愿偿还香甜可口的冰镇啤酒，就没有人愿意做他的朋友。

在情境2中，若其债务透过UCAC被记录在CP上，经济压力足以令其偿还债务—如果Jesse Corp无法兑现礼券，没有人会再去光顾Jesse Corp。

在上述2个案例中，特定的UCAC不仅可控管可被记录的债务类型，更具备内建的债务执行机制。一般来说，针对大型联锁公司亏欠权益较少的债权者，这种债务执行方式会显得格外有效。

由于法律和社会压力已无形中成为促使债务偿还的执行方式，CP的价值便在于其可透过双重确认去准确地记录债务。如此一来，目前社会上各方有关债务的繁琐程序便可予以免除。在区块链上记录有关债务可让个人和实体在进行债务交易时利用现有CP的机制，而无须经过银行、律师和其他信托机构的审批和处理。

以太坊复杂难解的难题

由于每一个被记录在CP上的债务/信贷交易仍将数据写入以太坊区块链，所以是需要使用以太坊支付必要成本(或称为gas)。虽然收费看似会大大减低CP的广泛应用，但BlockMason仍然相信未来的以太坊和其他数字货币将如同现今的现金一般获得广泛的认可。

随着网络新增区块链外(off-chain)处理和其他改善方案，以太坊网络的交易成本也将大幅缩减，相信在不远的未来，用户能以较低成本，便能使用DApp。[2] Vitalik Buterin和Joseph Poon近期宣布的Plasma更进一步证实了我们的信念，亦即以太坊很快地将可快速地处理大量的微型交易(microtransaction)。[3] 其亦证实了以太坊基金会(Ethereum Foundation)所做出的承诺，以太坊(Ethereum)不仅可用作一种货币，更可用作消费用的DApp平台。

除此之外，BlockMason早已开始研究其专有的区块链外解决方案，以便尽早予以实际应用。与其适应其他开发商的区块链外处理方法，我们致力于研发一个完全适合CP使用的区块链外，因为这是我们承诺会为维护和支持CP做出贡献。随着区块链应用程序日渐变得更具规模，用户将不会注意到他们每个月花在以太坊交易上的小额费用。

此外，BlockMason正在开发将以太坊钱包嵌入应用程序的的策略，以便为新用户支付其交易费用和吸引尚未熟悉加密货币的潜在顾客。例如，一项应用程序可为新用户自动产生一个以太坊钱包，而管理该应用程序的公司则可小额赞助用户的初始交易，并以之作为顾客获取(customer acquisition)的成本。如此一来，CP的相关应用程序便能降低技术门坎，从而推广区块链，使之成为技术主流。* * *

1. https://blockmason.io/blog/2017/07/01/introducing_foundation/ ↩

2. https://github.com/raiden-network/raiden/wiki/FAQ ↩

3. https://www.plasma.io/ ↩

Credit Protocol的使用范例：

我们可以一种最简单的方式来想象 — CP(Credit Protocol)是一个包括创造、追踪和结算借据(IOUs)的机制。基本上，借据与货币并无不同。最早期的现金型态，就是以金或银等贵重金属，或仓储谷物等商品做为标准化借据。**因此，CP允许个别用户去制定和控制客制化的借据，势必令加密货币发行的过程更自主化。**

因此，CP允许个别用户去制定和控制客制化的借据，势必令加密货币发行的过程更自主化**。**

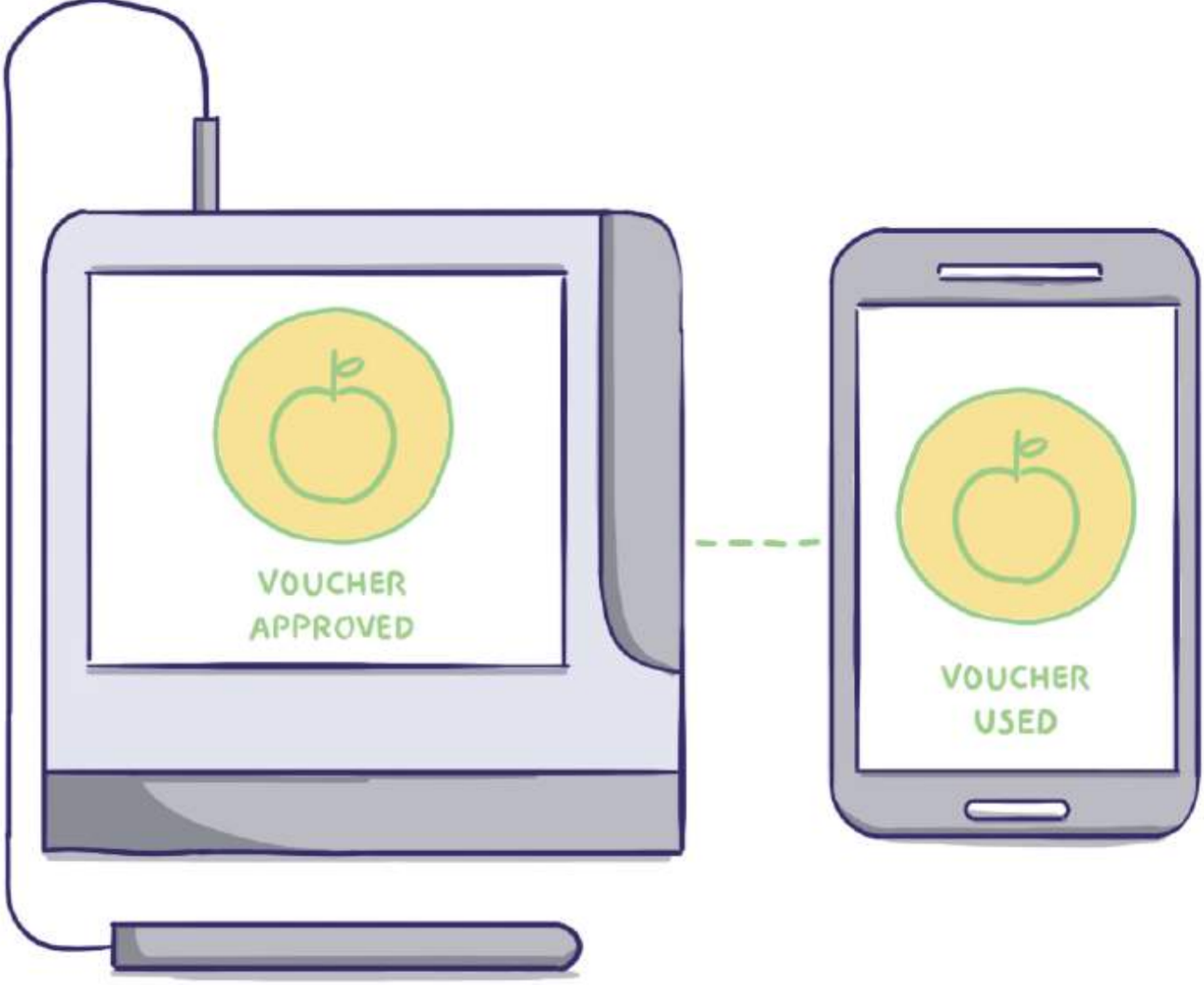
区块链外(Off-chain)已有相当广泛的借据使用案例—在厂商和买家之间以应收帐款(Account Receivables, AR)的形式存在，并在零售商和消费者之间以礼券的形式存在，在于航空公司和飞机旅客之间以里程数形式存在。有时，这些借据会以政府发行的法定货币(fiat money)作为结算工具；然而，其他情况下，借据的结算却只是采用其发行者随意选定的货币。只要双方信任发行者能以其他双方议定的方式赎回资产，所有借据都有其自身的价值。CP是一项实现这种广泛用途的基本工具，且所有持有CP代币(Credit Protocol Token, CPT)的用户都能使用和开发相关的CP工具。[1]

我们不难想象可在BlockMason的CP上建立功能多样化的应用程序数组的可能性。在以下章节中，我们将检视一些CP的应用案例—我们推出的悬赏计划 (参看下方解释)—以及我们推出的第一个CP应用：**Friend in Debt (FiD)** (Try It Now)。

我们邀请每一位对CP感兴趣者于 our github repository 检视其原始码。

大学餐券

我们可以想象一下，一间学校想为学生制定一项膳食计划。首先，学校需要购买足够的CP代币来应付预期所需的交易量。然后，校方会整合参加学生的Foundation ID名单，以防止非大学学生透过UCAC执行交易。UCAC经由此特殊设计，只允许校方和学生之间进行交易，以防止学生彼此私底下进行交易。餐券系统透过其免费的CP移转(transfer)功能 (与学校购买的CP代币数量成比例)，让学生得以结算有关债务，而无须在CP的网络上支付任何费用。接着，学生便可为膳食计划付款(例如：一个月$300)。学生可以用现金或数字货币向学校付款，而学校则可以向学生发送60个膳食代币。学生每次到学校食堂时，只需轻轻一触，学生即可使用CP直接记录及扣膳食代币付款。在学校的UCAC中，学校学生只能在校园特定的用餐地点进行交易。



小额融资

同样地，我们也可以参考上述的餐券系统，并以同样方式开发一套小额贷款系统。UCAC的创造者(在此案例下为放款人(lender))，可将每位借款人(borrower)的债务限额、多名借款人共同承担的单笔借款的还款责任(例如，来自同一社群或村落的个人)、借款利率、或还款时间表，全部一并写入CP合约。

此种小额融资是一种极为强大的工具，尤其是在一些没有完善银行系统的小区。它可以提升债务的流动性(liquidity)，并可在大型金融机构无法提供服务的区域内促进复杂的经济发展。此种类型下的开发应用可能包括小额商业贷款、低利息的发薪日贷款(payday loan)或集资偿还社群债务(crowdsourced repayment of community debt, 例如：在火灾过后共同负担重建业务或在意外后共同分摊医疗开支)。

零售礼券

另一个有用的CP应用：管理礼券(gift card)。消费者可以购买商店的消费抵用额，然后把抵用额存放在Foundation ID内，与商家建立债务合约。当消费者使用礼券去兑换一项产品或服务时，有关债务即可获得结算。

除此之外，用户亦可以从商家购买一个可被兑换的条形码，而条形码可以允许用户存取UCAC内的资金。在数字生态系统中，商家或消费者皆可灵活的发出和使用，从而简单地创造出类似Visa 现金卡等诸多实体，或可在一个特定商家的礼券管理账户中存放多种不同的礼券/抵用券。

由于各个商家的礼券使用方法极为相似，因此我们可以想象以一个整合统一后的应用程序，来管理任何数量的礼券，并可让用户将礼券赠予朋友，亦即将该礼券所属商家的债务合约转予朋友。

消费信贷

现时，申请消费信贷一般须经过相关金融机构的繁复审批，CP却能够大幅简化消费信贷审批的流程。由于区块链的分类账本(ledger) 有对外公开和受到保护的特性，因此用户可运用DApp来追踪其债务、透过第三方组织使债务偿还更加便利、确定能收回其贷出款项，从而避免发生债信行业中经常发生的诈骗问题。

此类系统亦可运用储存在CP的债务数据，并可藉此评估个别借款人的信贷和债务偿还历史。一份UCAC更可根据与该名借款人的FoundationID的信息，进一步验证借款人提供的数据之可信度。

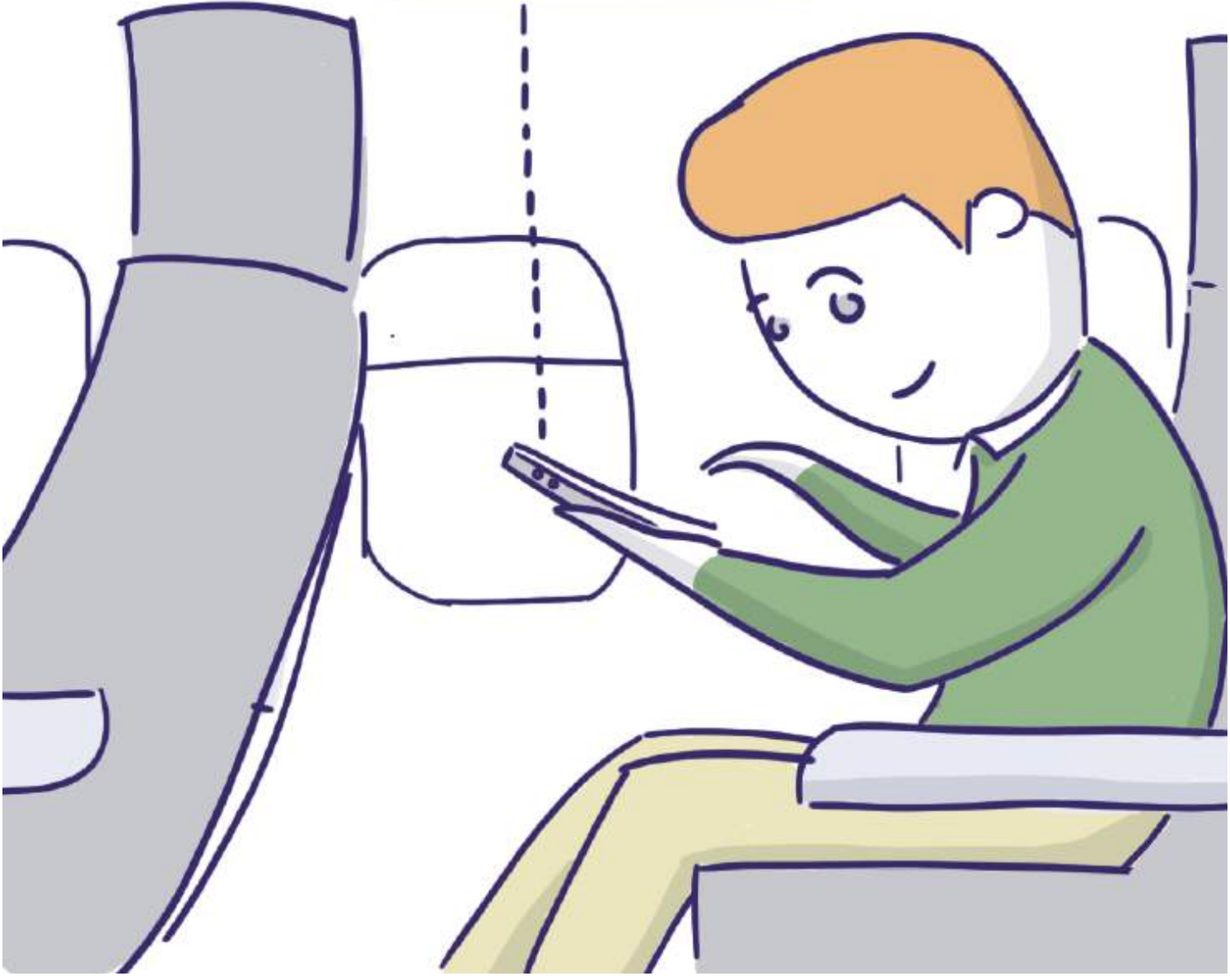
接到一通可疑电话告知您已迟缴车贷？您可以挂断电话，立即检查区块链以确认您的缴款状态。

航空旅行里程数/商家忠实度点数/信用卡点数

航空旅行里程数和商家忠实度点数是航空公司或商家与其顾客之间的另类债务型态。航空公司以其自身的货币(例如，IOUs)发行里程数，并根据其惠顾率为飞机乘客给予奖励。接着，用户便可根据航空公司或商家建立的点数系统索取有关产品或服务，以便结算债务。

此一厂商忠实度系统凸显出CP具的其中一个特性：债务无须以法定货币(诸如美元、欧元)或加密货币(诸如以太币ETH)进行记录。只要符合以下条款，用户可随意将有价值的货币地写入UCAC：

1. 能制定可行的赎回价值和赎回方法
2. 客户认为这新产生的"货币”(诸如航空旅行里程数或信用卡点数) 是具价值得



我们在此将最好的东西留到最后。

Friend in Debt

FiD是我们第一个推出的功能齐全的CP实作。用户可藉由此一社交工具，在朋友、家人和社群之间追踪和发行债务。其潜在应用和使用度相当广泛强大。我们非常期待能在本白皮书中的后续章节中为您详细地解释FiD。

然而，您也可直接跳往经济革命，并透过以下连结探索FiD： fiddy.io

1. 注意事项：CP的某些应用可能受到某些司法管辖区域的法规限制。CP的开发者须自行确认有关应用程序是否符合有关法规 ↩

为何采用Credit Protocol (CP)?

安全性

随着更多人开始使用以太坊(Ethereum)和其他加密货币来为规模较大的基础建设的开发提供融资，信贷业务必定成为生态循环系统中很重要和发展突出的一环。虽然个别处理数字债务可能会引申出缺乏保障的问题，但是我们会确保CP能通过层层测试并展现相应的可靠性。藉由CP(Credit Protocol)的运用，公司和个人得以免除对后端工程师的依赖。您只需要在UCAC订立适用的规则和一个前端接口，而完全无须担忧有关债务、信贷或资产的资料保密和安全性。

藉由CP的运用，公司和个人得以免除对后端工程师的依赖。您只需要在UCAC订立适用的规则和一个前端接口，而完全无须担忧有关债务、信贷或资产的资料保密和安全性。

便利性

随着CP发展出稳定的用户群，客户社群中将会有更多开发者和用户共同解决CP的操作问题，从而使CP上建立合约的过程将变得更简单且直接。很快地，UCAC的模板就能处理大小组织经常面临的各种财务问题。事实上，我们可以把此生态系统(ecosystem)想象成与网页模板类似的生态系统，一名潜在用户可在系统中搜寻到数百万种免费和付费UCAC的模板，然后根据个人需要加以应用。

规模

比特币已透过其数字信贷系统创造出一个全新的经济生态系统，如果无法把这生态系统的应用扩展至加密货币以外，这会局限了加密经济（crypto-economies）可发展的潜能。而健康的信贷和债务一般在经济发展中都当任不可或缺的角色。基本上，所有大规模项目和基础建设(包括桥墩、工厂、住家、技术创新)的开发都是由债务驱动的。事实上，世界最大的经济体 — 美国联邦政府 — 若无借贷和贷款的能力，可能在一夕之间倒台。发行债务的能力是数位经济增长的必备条件。

发行债务的能力是数位经济增长的必备条件。

除此之外，值得注意的是，由于以太币(ETH)来记录债务并不需要真正持有任何以太币，因此记录在CP上的债务和信贷总额很快地就会超过所有加密货币的市场总值。我们计划透过向开发者开放CP，从而加快这自住化工具的发展、市场渗透率和广泛使用率。

支援

操作新软件是一个艰难的过程。如果没有有效的技术支持，操作新软件可能使人历经数日的挣扎，但若能配合适当的技术支持，新软件可以为企业带来实时的解决方案。所以一个像CP的应用程序，成功与否和长期而言是否达到经济效益的关键，往往是在于有没有妥善的技术支持安排。

BlockMason透过CP的网站，会持续为顾客和代币持有人提供支持。有关资源包括不同的文件去解释如何利用CP增加生产力、如何将CP应用于各种案例和实际情况、以及一些成功项目和范例模板的例子。此外，我们还提供API 文件、UCAC样板和能够与UCAC功能融合的前端接口。简而言之，BlockMason将提供资源来引导顾客，以期从初始CP的运作概念转变成高效和实用的UCAC和前端界面。

最后，在BlockMason，我们并无"昆虫恐惧症”(entomophobia)。我们不怕系统漏洞(bug)；我们勇于修正各种系统漏洞。我们认真地看待系统漏洞报告，并为CP设置一套系统漏洞报告系统，从而使我们得以实时有效率地解决技术问题。

急迫性

在区块链上的债务和信贷活动是促成我们生态系统发展的关键因素。对此，BlockMason早已开发出一项有效可行的协议。您无需等待数年才能见到功能不全的解决方案。我们早已完成一个CP可用版本。我们在此邀请所有的潜在用户一同检视这生态系统的原始码。

Credit protocol illustration

CP的技术层面

Foundation的技术层面

请参看 Foundation Whitepaper，*以了解有关Foundation的详尽解释。*

请参看 Foundation Technical Documentation，*以建构有关Foundation协议(Foundation Protocol)的各项应用。*

BlockMason在CP早期未发行版的实验过后，便创造出Foundation。在开发过程中，我们遇到一些与身分识别(identity, ID)和钱包整合有关而目前在以太坊网络上的应用程序亦无法解决的的技术问题。例如，如果您想在桌面计算机上而非手机上存取一个基于CP的DApp，您会怎么做？您有需要冒险透过电邮将您私人的以太坊密钥传送给自己吗？您要将私人的以太坊密钥输入另一个电子货币包来汇入私人的以太坊密钥吗？如果您已决定使用新的以太坊地址搭配CP应用程序，您该如何将新的地址整合到应用程序之中呢？

透过无数的程序编写、多个不眠之夜和不断的尝试和修正，我们终于了解到，我们要的是一个可以在手机和桌面计算机上连结以太坊地址的整合机制。从我们最早开发CP的余烬中，Foundation就像凤凰一样浴火重生 —— Foundation存在的主要目的就是要让您所有的地址都能用Foundation作为您的身分识别。

Foundation的接口可让识别创造过程干净利落。您只需要一个与现存其他Foundation ID无关的以太坊地址即可。这很简单，在一名用户创造出一个Foundation ID后，该名用户可接着透过Foundation的智能合约选择新增其他与此一Foundation ID有关的地址。

此一整合统一的Foundation ID必须用到CP。用户可藉此维持单一身分识别，并可从任何装置和DApp浏览器存取CP。

Foundation Screenshot

CP资料智能合约

CP数据智能合约是实体之间"关系”及其”债务和信贷”数据储存的核心合约。其包括两个主要的数据结构：**关系(Relationship)和债务(Debt)**。

关系可追踪两个实体之间的关系。两个实体之间若要形成一项债务，两个实体就必须被界定为「相关联的(connected)」实体。除此之外，由于用户须确认关系请求，因此关系亦可追踪尚未确认的关系(pending relationships)。

债务可持续追踪一名用户和另一名用户之间的债务。此一功能可执行的任务包括追踪债务、保留未偿债务

数据、以及纪录特定债务计价的货币种类。

Credit Protocol智能合约

CP智能合约可读取和控制CP资料合约。此种合约的功能包括：读取用户债务、保留未偿债务数据、发送债务、确认债务、读取朋友清单、新增朋友、删除朋友等。

CP智能合约是可以控制CP数据智能合约储存数据的唯一地址。

用户只能透过Flux Capacitor合约(如下所示)与CP智能合约接合。

Flux Capacitor智能合约

Flux Capacitor合约是可与用户互动的合约。事实上，用户从未与UCAC发生直接的互动。Flux Capacitor合约的功能与CP合约的核心功能相仿，但唯一的例外是，每一个Flux Capacitor功能都会占用一个UCAC的地址。Flux Capacitor合约可根据UCAC地址上的UCAC来检查用户指令，以确保用户指定的参数值在特定的UCAC中确实有效。

除此之外，Flux Capacitor合约亦可检查投注合约(Staking Contract)，以纪录一名CP代币持有人(CP Token Holder)投注的代币数量，以及有关代币所揭示的合约项目。Flux Capacitor合约亦可指明该名用户投注代币可于特定期间内使用的剩余交易容量。合约可更新CP代币投注者的交易容量，并在CP数据智能合约中呼叫相应功能 。

我们可以简单地把Flux Capacitor想成一名强制执行者(enforcer)。其可根据一名用户为某一UCAC投注的CP代币数量来管理UCAC的参数并限制交易容量。

Use Case Authority Contracts (UCAC)

UCAC所包含的功能呼叫(function calls)，与Flux Capacitor合约所列举的功能呼叫完全相同。每一个功能都只会回传一个布尔值(true或false)。Flux Capacitor合约会在UCAC中呼叫名称完全相同的功能，以检查交易是否有效。

例如，Flux Capacitor 中的newDebt功能就会从UCAC中的newDebt功能呼叫与之完全相同的参数(bytes32 myId, bytes32 friendId, bytes32 currrencyCode, int amount, bytes32 _desc)。接着，UCAC就会回传true或false，以验证交易是否有效。因此，如果一个UCAC允许使用欧元而非美元，且一名用户试图透过Flux Capacitor合约传递美元，其布尔值就会回传false。若其回传值为false，就会导致Flux Capacitor中的newDebt功能呼叫失败。

UCAC可以有无限的理由回传true或false。唯一的要求是其必须和Flux Capacitor合约中的功能维持相同的功能名称和相同参数数值。若两者的功能名称和参数并不相同，Flux Capacitor合约的功能呼叫就会失败。

多名用户和投标喊价

在获得许可的情况下，多名用户可为相同的UCAC投注CP代币。如果一个DApp受到充分的欢迎，数以百计或数以千计的用户便有可能投注CP代币来帮助支持其交易。

除此之外，一个UCAC亦有可能写入相关规则，以允许CP代币的持有人透过其UCAC来争取交易。例如，2名用户可为相同的UCAC投注其代币，以2种不同的价格向UCAC用户公开发售其特定交易。接着，DApp便可以评估哪一个投标喊价最为便宜，并循该途径于发送CP交易前，向该用户提供报价。

投注智能合约

投注合约(Staking Contract)可储存一名用户投注在某一个UCAC的代币数量，从而驱使UCAC达成交易。当一名用户试图为UCAC执行一项功能时，Flux Capacitor就会去查询投注合约，以了解该名用户为驱使UCAC的交易达成所投注的代币数量。

除此之外，投注合约亦会监视一名用户的CP代币变化，以确保该名用户并未试图欺骗系统以取得免费交易。

技术层面的考虑

Foundation ID的命名标准

整合CP的Foundation ID只有在遵循小写字母和数字的命名标准时才会发挥用处。此一限制表示，Foundation ID若包含小写字母a-z和0-9以外的其他符号，就无法与CP一起发挥功用。

储存成本

在以太坊区块链上储存数据相当昂贵。为了让用户使用低成本的CP，BlockMason提供持续维护、支援、更新和优化产品等服务，以降低用户的使用成本。成本最小化是一个持续的过程。此一过程可能涉及到诸如IPFS等系统和其他区块链外储存解决方案(off-chain storage solutions)的运用。我们谨慎地选取变量类型(variable types)，以便将储存成本降至最低水平。同时，我们也小心地检视将特定数据储存在区块链上或区块链外的各种利弊。

可扩充性

尽管我们已对CP的现行版本感到兴奋，我们仍坚持提供最完善的维护和支持，包括在定期的版本升级中提供修正方案和扩展功能，以及高质量的软件服务。为了实践产品维护和支持的责任，我们将Foundation智能合约予以划分，以便将储存变量与实际功能做分割。如此一来，我们便能够更新协议的功能性并能维持现有的储存方式，从而节省将该储存方式置入新合约的成本。我们将为所有的CP智能合约都以相同的方式划分。

在以太坊区块链上建构应用程序的一大特性为"公开的分类账本”。由于以太坊网络上的所有人都能存取CP智能合约，因此未来的开发者亦可轻易地透过现有CP的基础架构上来建构新的应用。在此一透明性下，运用现有CP数据和功能性即可创造新的动态债务偿付模型(包括小额贷款、消费信贷和企业对企业之间的信贷平台)。

成本及经济效益

当BlockMason 设计CP(Credit Protocol, CP)时，我们可以将其想象成在全球范围内的每一个用户都能够免费存取的一种革命性协议。然而，计算机运算(computing)、数据储存(data storage)和交易执行(transaction execution)都会在以太坊区块链(Ethereum blockchain)上形成一笔成本。此成本通常被称作**gas**。因此，由于CP都在以太坊区块链上运作，因此使用此CP将无可避免地产生交易成本。加上，与使用网站托管的传统应用程序相比，其储存成本也相对较高。尽管我们相信以太坊(Ethereum)将无可避免地在全球各地取得主导，我们也了解到一般用户不一定需要理解以太坊及其运作方式。成功且可扩展(scalable)的去中心化应用程序(Decentralised Application, DApps) 可能将对一般用户来说是一件很普及但仅是在用户和以太坊网络之间设置多层(layers)的正常网页应用。

一般用户不一定需要理解以太坊及其运作方式。成功且可扩展(scalable)的去中心化应用程序(Decentralised Application, DApps) 可能将对一般用户来说是一件很普及但仅是在用户和以太坊网络之间设置多层(layers)的正常网页应用。

Plasma及区块链外(Off-Chain)交易

目前，整个区块链社群都在应对平衡成本和网络速度对比安全性和持久性的问题。幸运的是，我们似乎已能掌握一些改善方案。尤其是，近期发表的Plasma→^1 更展现出以太坊基金会(Ethereum Foundation)对于提升网络速度和减低交易成本的承诺，从而为消费者广泛地采用去中心化应用程序(decentralized applications, DApps)而铺路。除此之外，雷电网络(Raiden Network)，类似比特币(Bitcoin)拟议的闪电网络(Lightning Network)，承诺减少多达7倍的交易成本，并可于每秒处理多达100万笔交易。它将在区块链的一些交易转移到点对点(peer-to-peer, P2P)网络之中，且仍与以太坊网络(Ethereum Network)进行互动以保有其安全性和持久性。若智能合约(smart contracts)无法实行与雷电网络(Raiden Network)类似的解决方案，BlockMason将执行其自身的区块链外(off-chain)结算特性并让所有用户都能执行此功能。运用区块链外解决方案可让CP减少以太坊区块链的更新次数，从而减少相关成本。

最重要的是，我们相信CP将是驱使用户采用以太坊网络的重要因素。有关协议的能力和低进入门坎(low entry barrier)将有效吸引对加密货币不甚熟悉的新客户。同时，我们也计划设计CP的未来版本，以便代支新用户的交易费用，从而使新客户免去了解以太币和相关成本的繁琐。

CP将是驱使用户采用以太坊网络的重要因素。有关协议的能力和低进入门坎的特点，将有效吸引对加密货币不甚熟悉的新客户。

使用案例权限合约(Use Case Authority Contract, UCAC)、交易成本(Transaction Costs)和垄断(Monopolies)

CP代币(Credit Portocol Tokens, CPT)的持有人可根据其持有的代币(token)数量于每天进行特定数量的交易次数。尽管持有人可选择在其个人使用的CP DApss中运用其代币，以便使其自身的交易完成，代币持有人亦有可能追寻各种开发者途径。例如，持有人可投注于其掌控的DApp，以确保其用户能以持有人设定的收费或免费方式，透过现有的途径进行特定数量的交易次数。

代币持有人亦可选择将其资金投注在其他CP DApps，以便以有偿或无偿的方式为DApp的用户提供进一步的交易额度。例如，使用案例权限合约(Use Case Authority Contract, UCAC)可包括一套投标系统(bidding systems)，以鼓励CPT代币持有人为其用户提供途径。该投标系统可以多种方式写入，完全由UCAC的创造者自行决定；另还有一种解决方案就是透过一个公开的以太币市场(ETH marketplace)来争取最低成本的交易途径，并将其卖给DApp的用户。

这样的市场不一定需要基于相关费用来评估路径。相反地，软件可根据用户声誉(reputation of users)等其他因素来选择途径，即与CP完全无关的机构来加以决定。例如，一个环境机关可在区块链上证明某一CPT的投注持有人已采取对环境造成正面或负面影响的行动。接着，DApp就可根据该声誉选择是否透过该名用户的途径处理或不处理相关交易。一旦能够在区块链上评估用户身份特征，各种利用合约去评估用户互动可行性的场景将无限地出现的。

最后，由于UCAC可限制将其CP代币投注在特定合约的用户身分识别，因此CP代币 持有人完全可以为该合约创造实际上的垄断。例如，一间公司可能根据CP来建构一个DApp，但却只让其自身组织将CP代币投注在此一DApp。因此，该公司可在此一DApp中对有关交易收取任何费用，而无须担心其他CP的投注持有人会相互竞价。

上述所介绍的只是CPCP代币持有人在使用代币时能够追寻的某些行动和策略。

交易容量设定

每一个CPT可让其拥有人于每天处理特定的交易次数。每一个CPT所允许的交易数量可做动态调整(dynamically adjusted)，以便让其总交易量达到网络总体交易量的85%。

此算法监控(algorithm monitoring)和交易容量调整(adjusting transaction capacity)只会提升每一个CPT所允许的交易总量，而绝不会减少。此机制可保证可用的交易容量将随网络用量的提升而有所增长，并可防止买家因初始购买代币而失去可用的交易总量。这就好像在线数字影片和网络游戏的知名度增加后，将促使网络用量提高，从而带动宽带容量的扩张一样。

Friend in Debt (FiD) – 第一个CP的应用示范

着眼于以太坊世界的增长，BlockMason很自豪地向各位介绍一个让您可以随处和朋友在区块链上创造和结算债务的通用社交平台：**Friend in Debt (FiD)**。我们对它的描述为：

就像在区块链上的Venmo，只是更好

FiD不只是简化朋友之间款项支付的一项应用而已。如您所见，我们相信FiD可根据债务和数字货币，透过可信任的社交网络促发新的在地经济型态。FiD可成为个人金融借贷(尤其是无法使用传统银行业务者)的另一项选择，以便他们向社群内的成员进行融资，并建立跨越政治和地理疆界的经济结构，从而减少金融交易成本，并鼓励以太坊系统在全球范围内的发展。

在BlockMason，我们要您相信的绝不只是空泛的承诺；因此，我们邀请您 立即 参与FiD的现行版本测试 。即便FiD的beta 版本相当简化，我们还是希望您可以看见我们的愿景：建构一个去中心化的社交网络 (decentralized social network)，以便让大小社群都能轻易地进行债务追踪、放贷和信贷延伸。FiD可为社交借贷 (social borrowing)和小额贷款 (microloan) 带来一个新的强大系统，让您和朋友可以立即对此系统加以实验。然若非拥有可展现我们的目标和精湛技术并足以进行首次货币公开发售的实用产品，我们实也不愿浪费您宝贵的时间和精力。

最重要的是，我们相信区块链技术可让我们开发一项重要的应用——一个能透过社交网络内复杂的贷款和付款网络并让个人达到财务自由的应用。

我们正在建构一个全新的经济型态；一同加入吧! FiD 的现行版本。请 透过电邮传送 您的问题或意见。

不只是钱包而已：创造和结算社交债务 (Creating and Settling Social Debts)

我们都曾有过这样的经验：与不断借用洗衣房的邻居对质、帮助朋友偿还其跑车的贷款或分摊账单时与对方拳脚相向。FiD在本质上就是一种解决相关问题和拯救友谊的应用。同事之间再也不用为了谁该于何时付多少费用而争执不休了。不论是结算一系列的晚餐账单、收回前往国外的机票费用、或记录正式业务交易的发票，FiD都能为您处理各项交易。

除此之外，以具备交互式的朋友清单和债务列载机制而自豪的FiD，还结合了社交网络在财务弹性方面的吸引力。在此合伙机制与用户高度参与的前提下，系统将具有相当的可扩展性，而大小企业的交易效率亦可获得提升。与Venmo、WeChat Pay或Alipay等应用的不同之处在于：FiD可以简单的现场交易结算和立即的债务偿还带来更为复杂也更具效益的交易网络。

与Venmo、WeChat Pay或Alipay等应用不同之处在于：FiD可以简单的现场交易结算和立即的债务偿还带来更为复杂也更具效益的交易网络。

FiD的灵活性与筹资贷款追踪功能将可为各种规模的金融交易带来一种具革命性的发展。曾向银行请求贷

款的人都知道填写诸多表格导致手头抽筋或手腕发炎的痛楚、面对面遭盘问的窘境、以及等待信贷委员会批准的煎熬。而相对而言理应较容易申办的小额贷款(microloan)和极短期的发薪日贷款(payday loan)，却反而更容易被剥削(包括高利率和易使债务恶化的偿还计划)。又如信用卡申请，虽然申请时较少让人感到挫折，但申请过程也一样耗费时间和精力，而且没有人可以保证您一定可以取得理想的信贷限额。

反之，我们每天都与我们信任的人进行互动；彼此间培养起的信任远远超过我们与银行、信用卡公司或发薪日贷款行商彼此间的互信程度。在FiD问世以前，无论是追踪日常生活累积的小额社交债务、管理各方商定的大额贷款或监控社交债务等，都容易造成极为沉重的心理负担，也经常让人白费劲或导致朋友间因还款而发生争执；现在，FiD可让您更加轻易且轻松地透过朋友和同事等，进行融资。

诸如Venmo、Wechat/Alipay和各种加密货币钱包等应用，虽然宣称可减缓相关问题，其实却只能在现场交易结算时发挥作用—意即在面对较复杂的债务和付款的情境下，其功能性严重受到限制。此类平台不仅无法延迟结算债务、支付随时间增量的债务、或自动计算累加的利息，更无法长期追踪和结算债务。

除了以太坊钱包所具备的基本功能外，FiD还可让用户透过各种不同货币，去创造、追踪和结算债务，从而显著地扩张用户人数基础与应用实例；假以时日，FiD便可有效地在区块链上创造出一个去中心化的货币发行平台，并因「方便使用」及「与钱包相似的接口与功能性」而被广泛的采用。

FiD便可有效地在区块链上创造出一个去中心化的货币发行平台，并因「方便使用」及「与钱包相似的接口与功能性」而被广泛的采用。

BlockMason着眼于未来的发展和眼下的功能性，既而推出FiD。为了快速获取新用户的信任与背书，FiD可在搭载有Status和Metamask应用程序的浏览器之桌面计算机和行动手机上运作。除此之外，FiD将提供一个方便开发者使用且对外开放的后端应用程序接口(API)，以允许开发者建构其自身的前端平台，并将其前端平台整合到FiD。此一设置可让个别开发者存取相同的后端数据并创造许多不同的前端接口；而此一API的功能则可让具新功能新特点之平台更加平顺地落实于FiD平台之上。因此，若开发者在利用我们的平台时想到新的方法—诸如信贷追踪或交易评价—他们也能透过以太坊智能合约和FiD合约实现其自身愿景。

跨装置平台的统一登录

由于FiD可让用户长期追踪债务，并可让用户定期或随要求透过以太币进行债务清算，用户在决定如何发送和接收有关付款时的灵活性，极其重要。

和一般的以太坊DApps的不同之处在于，FiD运用BlockMason 的Foundation 协定 (Foundation protocol) (参看 Foundation Whitepaper)来统一跨装置和跨平台(iOS，Android和Web)的登录和身分识别凭证。我们的Foundation 协定具备可免除用户在多重装置和平台间转换的困难度与免除将私人密钥从一个电子货币包传递到另一个电子货币包的不便性等优点，Foundation协议是我们计划优化用户接口和大幅提高被广泛采用程度的重要组成部分。

我们为用户降低技术层面的进入门坎，以期能改善用户体验并提升用户对FiD DApps的需求。更重要的是，整合的Foundation 协定可让FiD轻易地透过临时的以太坊网络地址新增潜在用户，并于稍后在不影响原FiD账户的情况下将该用户转往其他电子货币包。

降低技术层面的门坎

FiD利用BlockMason的Foundation协定和CP，将各个用户钱包的地址整合到相同的ID之下，从而成功地解决了最重要的技术层面门坎。整合后的账户可让用户更加轻易地登入多重账户、钱包和平台，而无需透过繁琐却不安全的方式发送私人密钥。同时，Foundation还可以让用户选择透过以太坊进行债务结算时，更自由与轻易地在多重地址之间进行转换。

安全性更佳

FiD不仅在用户接口和功能性方面改善了现行的付费应用程序，更大幅提高了现行付费应用程序的安全性。举例来说，Venmo的使用者账户就特别容易受到罪犯所盗用。

2017年7月19日， Verge 对外公告了一名Venmo窃盗犯的案例。该名罪犯在洛杉矶的窃盗了价值达US$25,000的相机设备： The Verge: Venmo Scam - Fake Payment Merchant Clause Fraud

与一般人的认知有所不同的是，在Venmo上的交易不会立即生效。款项可在已被注记为成功移转到另一个Venmo 用户的帐户后，仍可加以取消或撤销。尽管Venmo为发送款项的用户提供诸多保护，Venmo却为收取款项的用户提供极少保护。如文章内所言，付款方可能以遭盗窃的信用卡或银行卡向收款方支付费用。Venmo首先会冻结受害者的账户，拒绝他们存取其现有的余额。接着，Venmo会告知受害者，因其以商品兑换金钱之行为违反了Venmo的用户政策，既而无法获得任何实际的补偿。

与一般人的认知有所不同的是，在Venmo上的交易不会立即生效。款项可在已被注记为成功移转到另一个Venmo 用户的帐户后，仍可加以取消或撤销。

Paypal是 Venmo的所有权人。众所周知的是，Paypal经常冻结用户在其帐户内的资金，并随意将用户踢出平台。Venmo 还会因为用户付款时加上玩笑性十足的交易描述，为其冻结用户的帐户。 Angelina Travels: Venmo Account Frozen

在FiD中，用户无须担心其帐户会因为开玩笑或其他因素而遭到锁定。由于FiD 透过以太坊来结算有关款项，相关款项都受区块链的安全保护，因此，即便是大型机构或任何第三方机构等，都无法对用户构成威胁。FiD的顾客永远都能存取其资金、透过以太坊结算其自身债务、并可支领协议规范内的信贷额度，既而降低非现金交易所需面临的各项风险。

在FiD中，...相关款项都受区块链的安全保护，因此，即便是大型机构或任何第三方机构等，都无法对使用户构成威胁。

FiD 的Beta版本

FiD现行版本已可运作。尽管此一新版软件仅为相关应用的未来样貌提供精简的样板，FiD beta版却也展现出BlockMason对DApp的承诺。我们是真实相信我们现有的产品，而不只是单凭一本白皮书和一些空泛的承诺，就进行ICO；因此，在ICO期间，我们将持续公布重要更新，以扩展与增加FiD的功能。

目前，FiD 保有一份朋友清单，并允许新增、确认和清偿有关债务。Ropsten TestNet存有已发生之各项交易，从而可让用户存取testnet Ethereum及与相关应用程序进行完全免费的互动。beta 版本可于Chrome中运行，但须搭载Metamask。 fiddy.io image alt text

未来版本

BlockMason每天都致力于FiD的进化。我们计划在来年中公布多种新的版本，以扩展其功能性。未来期望新增的功能列表，如下所示：

- 结算各以太币钱包之间的债务并于并于债务的本国货币和以太币之间设有自动转换功能。
- 群组结算特性。朋友可加入一个群组、新增共同债务、并在群组成员之间分割相关债务。
- 创造债务偿还计划，可让用户管理贷款，并以简单安全的方式偿还债务。
- 自动偿付重复发生的债务，诸如每周的园艺工作、小孩的零用金或赡养费。
- 区块链外结算债务(off-chain settlement of debts)功能，以提升网络速率并减少交易成本。

Friend in Debt (FiD) – 市场机会：

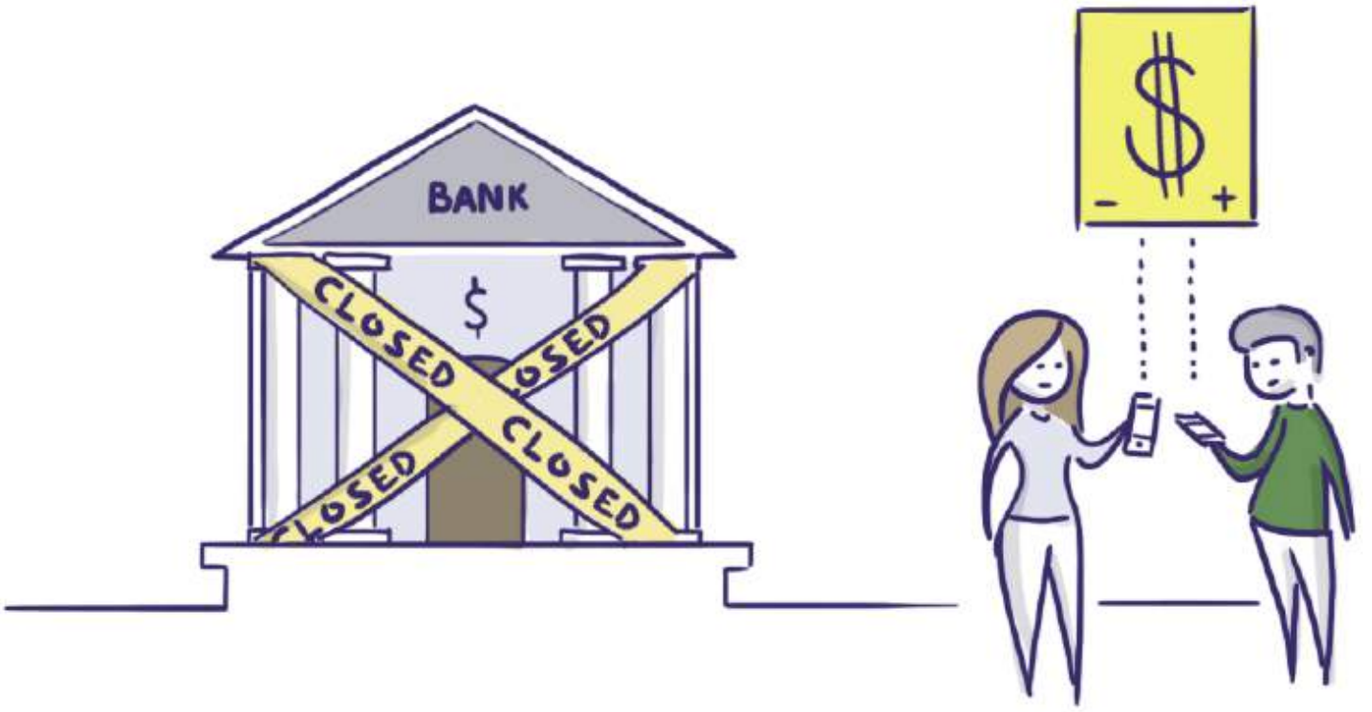
使放款人的角色更加自主

对借款人和放款人来说，FiD是个应用广泛的强大工具。如前所述，FiD 可让每一个用户随时随处担任其朋友的放款人；而对于特定无法使用一般银行业务的人，透过FiD，他们不仅可以建立信贷额度，更可以个人的名义对其同事发放信贷——自己本身就能有效地执行银行业务。由于FiD 免除了传统银行业务的企业管理费用，因此放款人和借款人可避免限制性成本和不断变化的规范，从而促进社交网络中的自由交易。

为无法使用银行业务的人提供银行业务服务

身处于较为富裕的经济体中，银行的普遍性及普及化，致使多数人无法想象无银行体系或无信贷体系的生活。然而，在东南亚、非洲、中东和拉美等区域，其金融劣势为区域经济带来负担、限制财务增长、并且阻碍个人行使金融交易的权力。

虽然使用大型金融机构的机会相对较少，这些地区的大部份人/机构却用着可使用应用程序的手机来存取数据和存取wifi。对于这些人而言，他们就愿意用安全且数字的方式(或透过其手机)来管理个人财务金融与金融借贷，这正为FiD大幅增加了市场机会—例如：东非兴起了一种在规模和效率方面远比FiD差劲的系统—「 手机微货币。



即便是在银行业务普及的国家，许多机构都不如美国提供的自动结算所 (Automated Clearing House, ACH) 系统来得便利。需存取银行账户的Venmo 虽然在美国部分区域受到欢迎，但却无法在美国以外的地方使用。同样地，尽管Wechat Pay和Alipay在中国已十分普遍，这些系统几乎只有中国人才会使用。

一般来说，世界上现有的金融交易系统都会要求用户支付转账费用。少数致力于改善金融流动性的手机应用程序要求用户自身需要拥有银行户口，且受限于市场覆盖率，足可见市场对FiD等与加密货币有关的金融交易应用程序实有巨大的需求。FiD不仅是加密钱包，FiD不会复杂到令一般用户难以采用，FiD的接口方便用户使用，建立帐户的过程也十分简单。

FiD的技术层面：

CP智能合约

CP智能合约是FiD得以运行的基础合约。FiD或多或少可被视为一种不受限制且以CP作为基础的UAUC。前述和CP背后机制有关的各项描述，都能在FiD中加以适用。

Foundation是用户与FiD进行互动的核心。意即，为了使用FiD，您有必要取得FoundationID，而相关FoundationID均能透过目前免费的Foundation的管理者用户接口来轻松创造。

FiD的UCAC

FiD的UCAC基本上并无任何规则。意即其对一般大众开放，且对其可通过的债务金额未设限制。

FiD的UCAC要求用户先用以太币购买CP代币。CP代币持有者可以利用CP代币从主掌用户竞投所需的交易次数。FiD的UCAC将为其用户自动选择最低价格的交易，从而确保成本尽可能地低。因此，在非免费交易的情况下，FiD的用户必须使用以太币支付一笔交易金。另外，尽管FiD的现行版本要求用户持有以

太币，BlockMason仍计划于未来为没有以太币钱包的新用户提供其他支付方法，进而使潜在客户的人数大幅提升。

Market Handler

FiD的UCAC实行一套智能投标系统，使CPT投注者对支持FiD的用户交易进行投标。实用上，CPT投注者将投标一笔特定金额的以太币，以作为其欲对进行相关交易时所应收取的费用。若其投标标案仍有剩余的交易容量，最低投标价格(对FiD用户来说最为便宜者)将可胜出。

一开始，BlockMason将搁置部分CP代币并将其投注到FiD交易上，以便让用户进行免费的交易。未来，BlockMason将评估是否继续使用此一手法、使用较少的信用协议代币或提高有关交易价格。

Front End

FiD的front end是以Purescript写成。Purescript是一种包含表达性的强大静态型别语言。Purescript可被编译为javascript又极其类似Haskell。我们喜欢Purescript的原因在于其进阶型态系统可让我们制作雏形并做更加快速地进化。这些特质都能确保和提高在Purescript中编撰程序的便利性、趣味性，并可大幅减少系统出错。

在不需要拥有实际技术专长下，front end 令用户可以轻易与智能合约的功能结合。同时，front end亦可以方便用户以简单检视的方式来显示数据。

image alt text想取得有关front end的更多信息？何不亲身尝试?FiD beta版本已可下载， 欢迎试用 。

总出售期为30天。出售目标为45000ETH等价的代币。Credit Protocol Token (CPT)的总发行量是91901211 CPT，发行后不会有更多的代币发行。在ICO的过程中，BlockMason会将55140727 CPT以1ETH对比1000CPT的对比率出售。而且根据购买的时间，购买者会有最高达到百分之五十的免费赠送。赠送的代币会从总发行量中扣去。任何没有出售的代币会被保留在未来发行。

Pre-ICO Period (50% Token Bonus)

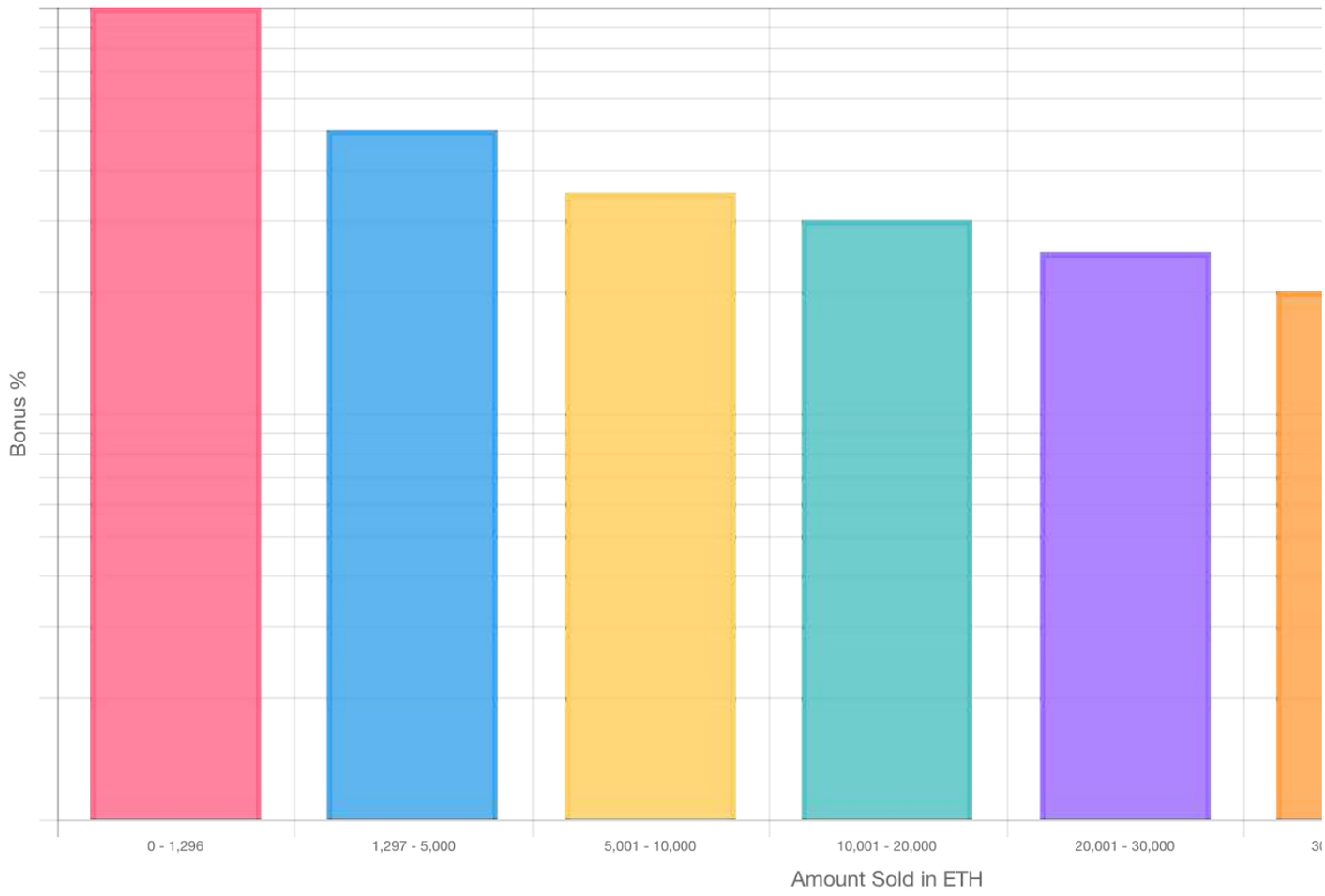
BlockMason充分认识到许多ICO中存在的问题，比如小买家在ICO期间未能获得购买代币的机会。因此，BlockMason提供了保证，不管大小，将代币分配给CP的的早期用户，即在ICO之前购买代币的人。这一窗口为所有潜在客户提供了一个机会，以保留代币的采购机会，而不同于其他ICO中“鲸鱼”和黄牛垄断了大量的分配，挤压了较小的购买，并从转手代币中牟取暴利。BlockMason会记录所有请求有保证机会的用户的以太坊地址。通过对ICO监管的智能合同的执行，每一个要求分配的地址都保证能在最初2天内购买cpt(而最低购买层不含额外代币)。在严格上限之外，在ICO前期，没有客户购买的上限。

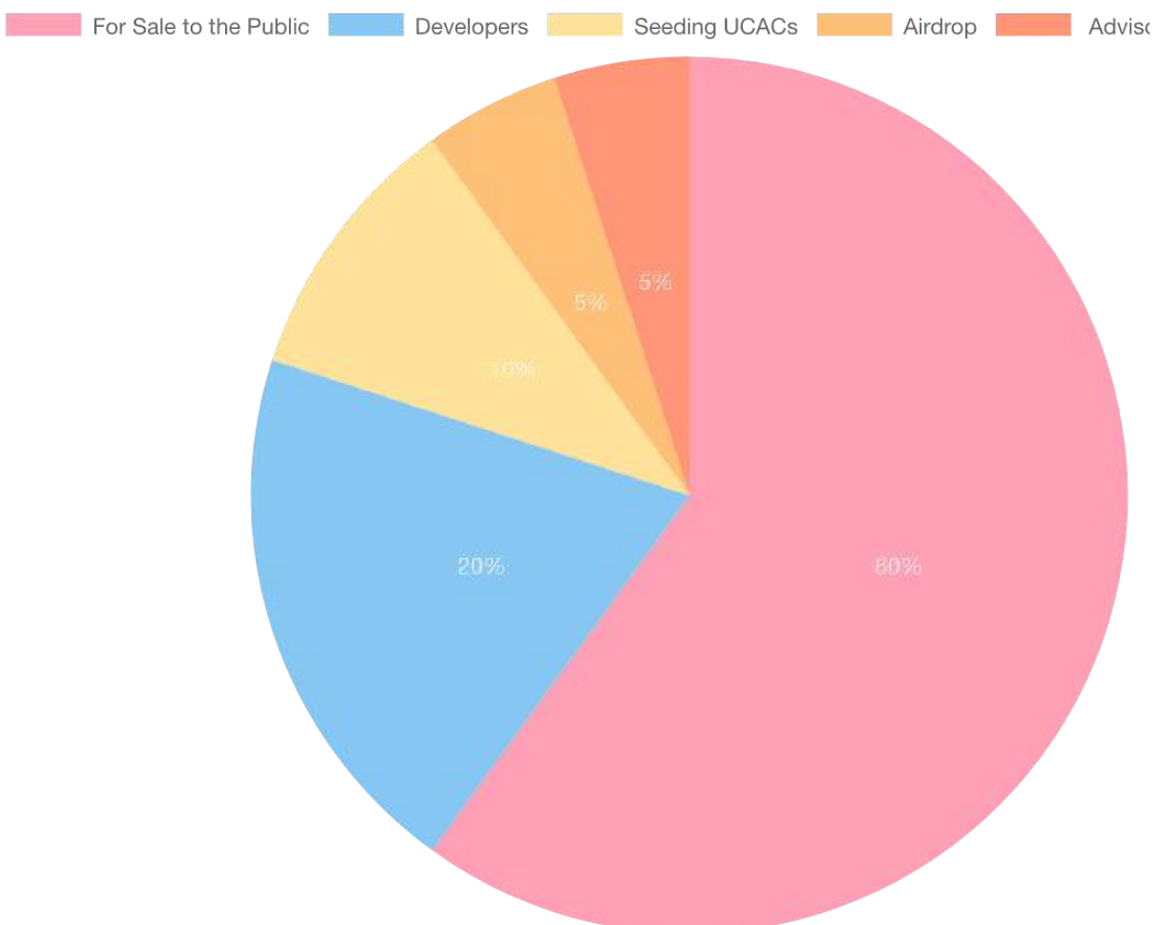
代币销售机制

在正常的ICO期开始时，在ICO前期阶段所做的所有采购将立即计入在奖金池数(见下图)，并按其收到的

顺序按时间顺序排列。在ICO期间所做的采购将根据他们完成的顺序获得奖励，并在所有ICO前期客户之后继续执行。例如，如果在ICO前期销售了20,000ETH，在这种情况下，下一个购买者将会获得15%的CPT赠送。

赠送结构





资金运用及发展规划

BlockMason已为首次货币公开发售(Intital Coin Offering, ICO)的收入运用和分配制定了一项特定、具体的计划。根据信用协议代币(Credit Portocol Tokens, CPT)的购买总量，我们将透过以下方式执行我们的开发计划。我们的支持和维护计划不仅包括重要的文件纪录和顾客支持，更包括将友人债务(Friend in Debt, FiD)置入其他操作系统和使用案例权限合约(Use Case Authority Contract, UCAC) 的开发，以供顾客能在信用协议(Credit Portocol, CP)的各种实作中加以运用。我们将持续更新和推进FiD，并以此作为CP的开放原始码范例。我们想要重申的是，BlockMason已对外发布有关 CP及FiD 可用的测试(beta) 版本。我们邀请各方考虑参与此ICO的同时也能对有关软件进行测试。

- **若售出2,250,000 个CPT **– 制作Chrome Metamask 的Friend in Debt Application (FiD App)完整版本和行动网页应用程序(Mobile Web App)。内部将开发出1个UCAC智能合约并免费提供给CPT顾客。CP的支持文件、部署指南(deployment guides)、UCAC建构范例(construction examples)和部署指示(deployment instructions)的供应将与CPT的发售数量成正比。(如果我们未能销售至少2,250,000个CPT，如上所示， CP ICO智能合约将自动把所有的以太币退回到以太坊的来源地址)；

- **若售出12,500,000个CPT** – 制作Chrome Metamask 的FiD App完整版本和行动网页应用程序。将一般的债务结算功能写入CP。FiD加入把所有主要加密货币债务结算功能。内部将开发3个UCAC智能合约并可免费提供给CPT的顾客。CP支持文件、部署指南、UCAC合约建构范例和部署指示的供应将与信用协定代币(CPT)的发售数量成正比。

- **若售出25,000,000 个信用协议代币CPT** – 制作Chrome、行动网页应用程序、 Andriod和IOS的FiD Apps。将一般的债务结算功能写入CP。FiD加入把所有主要加密货币债务结算功能。内部将开发5个使用UCAC智能合约并可免费提供给CPT的顾客。CP支持文件、部署指南、使用案例权限合约建构范例和部署指示的供应将与信用协定代币(CPT)的发售数量成正比。

- **若售出50,000,000 个CPT** – 制作Chrome、行动网页应用程序、 Andriod、IOS、OSX、Windows和Linux 的FiD Apps，并配备完整的以太坊钱包(Ethereum wallet)功能。将一般的债务结算功能写入CP。FiD加入把所有主要加密货币债务结算功能。内部将开发7个UCAC智能合约并可免费提供给CPT的顾客。CP支持文件、部署指南、UCAC建构范例和部署指示的供应将与CPT的发售数量成正比。

- **若售出75,000,000个CPT** – 制作Chrome、行动网页应用程序、 Andriod、IOS、OSX、Windows和Linux 的FiD Apps ，并配备完整的以太坊钱包功能。将一般的债务结算功能写入CP。FiD加入把所有主要加密货币债务结算功能。UCAC写入计息信贷功能。内部将开发10个使用UCAC智能合约并可免费提供给CPT的顾客。CP支持文件、部署指南、UCAC建构范例和部署指示的供应将与CPT的发售数量成正比。

- **若售出175,000,000 个CPT或更多** – 制作Chrome、行动网页应用程序、 Andriod、IOS、OSX、Windows和Linux 的FiD Apps，并配备完整的以太坊钱包功能。将一般的债务结算功能写入CP。FiD可以把所有主要加密货币债务结算。UCAC写入计息信贷功能。区块链外(Off-Chain layer)会大幅缩减信用协议(CP)的使用成本。内部将开发15个UCAC智能合约并可免费提供给CPT的顾客。CP支持文件、部署指南、UCAC建构范例和部署指示的供应将与CPT的发售数量成正比。

以下清单概述了为特定用途的收益配置。收益配置的上限和下限的百分比可反映出：我们出售越多的代币，就越能将其收益配置到营销和顾客支持。但我们当然也得为更多的顾客提供支持！

- **平台及应用开发 (35-50%)**：包括软件开发、 为ICO结束后的6个月内在多个平台上推出FiD而开发之团队的薪水；
- **行政管理、法律和营运开支 (5-30%)**：包括薪水、办公室、文具、家具、硬件、和法律、会计及相关的专业费用；
- **营销和顾客获取(5-20%)**：包括点击付费(Pay-per-Click, PPC)、广告展示、搜索引擎优化、内容营销；
- **顾客支援 (10-20%)**：包括文件记录、智能合约维护(smart contract maintenance)、范例、应用程序示范(demo apps)、front end插件指示(front-end hook-in instruction)、电邮和聊天支持；以及
- **额外奖励金总量(Bounty Pool) (5%)**：类似于领先科技公司的安全漏洞奖励计划。 为了在对客户群造成不利影响之前找到关键的安全漏洞。 包括UCAC开发商的奖励金。

营销计划

尽管我们相信以太坊社群(Ethereum Community)采用的是公平合理的菁英领导体制，以便让最为强大、有用的应用一跃成功， 然而我们也知道开发软件只是建构一项成功产品的一小部分而已。应用程序营销(Application Marketing)虽不比产品本身重要，却仍是所有公司的重要任务。共同创办人Timothy Galebach和Jared Bowie都在科技营销和社群参与方面产业都具备有多年的经验。他们在营运点击付费应用程序的广告活动，拥有深度的知识，也激励我们将FiD从只是一个随机的区块链应用(blockchain application)转变成一个主流的应用程序，并高居应用程序商店的排行榜。

Tim和Jared 均已为自身开发出可用于广告追踪(advertisement tracking)和优化配置的专属软件。更重要的是，透过他们多年在网络广告空间的工作经验，他们更开发出一个广纳专业人士的网络，以便做最有效率的营销广告活动。这包括大规模的广告购买、运用鼓励安装应用程序的机构、或从事横幅(banner)和登录页面设计的合约制自由工作者(contracted freelancers)。

CP和FiD的开发路线图

日期	特性	描述
2017 Q2	内部将ALPHA 版本部署到 主网络（MainNet）	内部概念实证Beta版本部署到Ropsten和Mainnet并提供Metamask 支持。
2017 Q3	完全重写 V1.0.0	Chrome Metamask FiD的Alpha 版本1.0已于Ropsten对外发布进行私人测试。
2017 Q3	发布备选方案	发布备选方案。Chrome Metamask FiD的版本1.0 of已于Ropsten对外发布进行测试。
2017 Q3	宣布首次货币公开发售(ICO)	信用协议(CP) 首次货币公开发售(ICO)， 以便为FiD提供推进力道。
2017 Q4	主网络（Mainnet）部署，版本2进入测试阶段	在主网络（MainNet）上部署合约。可支持结算的新一代合约将部署到测试网络（TestNet）。
2017 Q4	FiD部署到手机应用程序的浏览器	FiD 经由完整测试，至少能在一个手机应用程序的浏览器上运作。
2017 Q4	基础开发者文件和UCAC可供使用	记载如何使用CP的基础文件记录。另一个全面运作的UCAC以提供不同的CP使用案例。
2018 Q1	通用结算功能（General Purpose Settlements）启用	通用结算功能（General Purpose Settlements）将部署到主网络（MainNet）。
2018 Q1	桌面计算机应用程序进入BETA测试阶段，手机应用程序对外发布	桌面计算机应用程序 Beta版本对外发布进行测试， 应用程序于Android和iOS各自的商店上架。
2018 Q1	经过改善的开发者文件和提供更多的UCAC	与CP运用有关的详细文件记录—包括UCAC范例、部署指南和基础指南。提供5个功能齐全的UCAC。
2018 Q2	版本3进入ALPHA测试阶段，桌面计算机应用程序对外发布	桌面计算机应用程序对外发布。版本3进入ALPHA测试阶段。附息贷款智能合约于测试网络（TestNet）对外发布。
2018 Q2	版本3进入BETA测试阶段，贷款合约部署到主网络（MainNet）	版本3已对外发布进行Beta测试。计息信贷合约部署到测试网络（TestNet）。
2018 Q2	经过改善的开发者文件和提供更多UCAC	与CP运用有关的详细文件记录—包括UCAC范例、部署指南和基础指南。提供7个功能齐全的UCAC。
2018 Q3	附息贷款写入FiD	计息信贷功能写入FiD。
2018 Q3	区块链外交易管道进入ALPHA测试阶段	内部开发的交易汇聚和快取层（aggregation and caching layer）进入Alpha 测试阶段。
2018 Q3	经过改善的开发者文件和提供更多UCAC	与CP运用有关的详细文件记录—包括UCAC范例、部署指南和基础指南。提供10个功能齐全的UCAC。
2018 Q4	版本3对外发布	版本3对外发布。其中包括附息贷款和链外交易管道带来的大幅缩减的交易成本。
2018	经过改善的开发者文件和提供更多	与CP运用有关的详细文件记录—包括UCAC范例、部署指南和基

安全性

撰写以太坊的程序代码是一项全新的复杂工作。由于其新颖性和确保未经测试的程序代码具备100%的安全性有其困难度，以太坊社群已于近期蒙受许多大规模的黑客入侵。BlockMason致力于避免可能损及名誉的错误。我们已采取以下步骤来确保有关应用和首次货币公开发售(ICO)的安全性：

- 根据最佳实践写入安全的程序代码。
- 慢慢地推出新的产品特性和改善方案。首先于局域网（Local）进行，之后再前往测试网络（Testnet）或甚至是主网络（MainNet）。
- 以专业的方式审查所有与以太坊或信用协议代币(CPT)发生互动的程序代码。
- 提供漏洞赏金（bug bounty） 以鼓励白帽黑客（whitehat hackers）找出并消除程序错误。
- 运用 ENS 地址、首次货币公开发售(ICO)前发布ICO 合约、以及建立清晰安全的沟通管道。

各该步骤都是我们通往终极安全计划的开始步骤。BlockMason不断研究和评估其他DApp公司面临的各项威胁，并对我们的安全性措施做出相对应的调整。我们已将大量的时间、精力(和爱)投入到CP和 FiD之中。若有严重的安全性问题，我们可能因此而万念俱灰。我们的声誉和你的信任可能因此而处于危急状态。因此，我们将以最为谨慎小心的态度来处理各项安全性问题。

常见问答集

在区块链上各项交易都是透明化的。我该如何确保交易历史能有一定的隐私性呢?

尽管目前在区块链上的交易纪录都是对外公开的，以太坊基金会(Ethereum Foundation)和ZCash(一种匿名性的加密货币)的团队正在合作开发 Project Alchemy，以便提供匿名的区块链交易。最终，只有发送方允许的特定用户才能看到各项事务数据。在启用此一协议后，所有有关公开和可见交易的问题都将消失。在以太坊现行的版本中(Homestead)，各项事务数据都是对外公开的。因此，用户只应张贴其愿意分享的事务数据。

在区块链上发送交易不是非常昂贵吗?

若与比特币、银行转账或信用卡等其他选项相比，如果在以太坊网络上只发送以太币作交易，其交易成本就会非常低。但另一方面，储存债务，放款人，借款人，和货币等数据就会明显地较昂贵。

我们的首要目标之一就是要降低交易成本。在我们理想的Credit Protocol (CP)版本中，用户根本无须考虑交易成本。在更好的情况中，用户更加无须明了以太坊的复杂运作和交易成本的定价方式。系统成本将尽可能保持在最低状态，以便让一般用户得以轻松采用。

我们将采用如雷电网络 (Raiden Network)或内部自行研发的区块链外解决方案来大幅缩减交易成本。区

块链外解决方案可缩减交易成本达100倍。

以太坊网络不是很慢吗?

以太坊基金会(Ethereum Foundation)的主要目标之一就是要大幅提升网络速度和可扩展性。在未来，以太坊不太可能不能直接在区块链上或区块链外透过网络如Raiden等轻松于每秒完成数万笔或数百万笔交易。与此同时，以太坊的未来销售点(POS)系统据称可以每3秒一个区块的速度进行区块挖矿。Raiden和其他现成的链外解决方案，则承诺可带来更快的速度。在网络扩展、Plasma区块链技术和链外交易选项的开发之间，以太坊网络将有可能见证交易速度的大幅提升。这可是 DApps获取大量用户的关键步骤。

如果一名用户的地址遭到黑客入侵， CP和 FiD会发生什么事情?

不幸地，黑客入侵是目前已开发的以太坊生态系统所需考虑的现实。我们完全了解以太坊用户面临到的各项威胁，也已投入了大量的时间来顾虑Foundation 用户的安全性。为达此一目标:

CP和 FiD不会持有任何以太币。因此，骇入CP或 FiD用户帐户不会带来任何的以太币得益。以太坊将如往常般地储存在用户钱包或地址之中。

债务须由发送方和接收方确认后，才能达成交易。遭骇账户无法发送债务或支付款项。

债务结算需手动完成，且须始于某单一地址。此一地址及其以太币具备充分的安全性，且与其他Foundation 账户相互分离。其为一个正常的以太坊地址。

Foundation协议(Foundation Protocol)智能合约可将数据与逻辑分开。在我们审查安全性时，我们也能更新Foundation而无须丧失用户的基本数据。Foundation是CP的必要组件。我们期待大家一同检视其公开的原始码，以便持续改善其安全性。

若其余代币未透过代币公开发售发售出去，又会怎样呢?

首次货币公开发售(ICO)期间未能出售的其余代币将由BlockMason持有，并可于未来的代币公开发售中加以出售。BlockMason欲持有20%的CPT供应量，并将额外的 10%投注在BlockMason开发的FiD和其他CP示范应用。

若朋友不履行其债务，又会怎样呢?

FiD并未为金融交易提供保护。对于不可信任的朋友，我们只能建议您立即结算有关债务或避免扩张其信贷限额。

我们不会对您的友谊加以裁断—我们的工作人员有限。他们无法随传随到。

团队简介

Timothy Galebach (共同创办人)

Timothy是新创公司的创办人、技术专家和业务开发专家。他特别专注于数据驱动的风险投资和自动化基

础设施。他目前是Almond Media Solutions(专攻电子商务和展示性广告营销空间的技术咨询公司)的所有权人兼创办人。

Timothy于2007年毕业于哈佛大学（Harvard University）。他取得了计算机科学的学位并与多家新创公司和成立悠久的公司合作，并担任首席技术官的职位。他主要为销售人员和内部业务团队在可视化和可行动化上呈现大量数据，并透过积极的优化和自动化数据编配为其节省成本。

Jared Bowie (共同创办人)

超过10年来，Jared Bowie均致力于设计各项系统来协调分布式数据库和点对点网络(peer-to-peer network, P2P network)。他是比特币的早期采用者，并已投资多种竞争货币的挖矿作业。当他开始在其区块链上撰写程序时，他便对以太坊的力量感到着迷。现在的他也相信其力量终将风靡全世界。

Jared毕业于詹姆斯·麦迪逊大学（James Madison University），主修哲学。毕业后，有感于大数据和展示性广告营销的汇聚趋势，他创立了一家数位广告风险投资企业。自此，Jared 便开始撰写专业软件和专属算法，并成功地运行数百万元的广告活动和管理位于香港、中国和印度的团队。

Michael Chin (共同创办人)

Michael 以极优异的成绩毕业于圣路易斯华盛顿大学（Washington University in St. Louis）。其主修金融和会计。他的职业生涯皆投入在信贷产业之中。一开始，他在纽约J.P.Morgan里的次级信贷部门工作。Michael接着转往J.P.Morgan在香港的债务资本市场和杠杆金融部门，帮助亚洲的公司进行投资等级、高收益债务、和联合贷款等债权募资。接着，在帮助成立了BlockMason之前，Michael加入了Intermediate Capital Group(欧洲次级债务的先锋公司之一)的香港办事处(FTSE 250企业中的其中一家企业)。

Luke Zhang (开发主任)

Luke是一名经验丰富的软件开发者和设计师。其以往的成就包括建构一项可处理数百万元开销的自动化广告工具。他还参与设计一套横跨全球系统，以追踪供应链上的产品组件，每年处理金额超过$4000亿元。曾在加拿大和中国受过教育的Luke自2011年开始便热衷于区块链技术。自此，他便非常享受有关如云霄飞车般的科技演进。Luke一生致力于开发以太坊网络应用，但他如今已不在人世。

顾问

Jesse Nee-Vogelman (内容大师)

Jesse是他那一代的最佳代言人。他于2013年毕业于哈佛大学（Harvard University），主修斯拉夫语和文学。他在学期间的最后2年在哈佛玉玺学会担任艺术家，完成了一部小说。此前，他在南韩和美国担任自由工作者(撰稿人)和撰稿顾问。他的小说已于The New Haven Review(新港评述)和The Harvard Advocate(哈佛之声)公开出版，并因此而赢得了贝格雷奖（Louis Begley Prize）。他在Pretty Much Amazing、Slant Magazine、Spectrum Culture和The Daily Distiller均有音乐评论特刊。此外，他也非常喜欢猫和狗。

Teddy Ninh (原创艺术)

Teddy Ninh 是一名年轻的艺术家 。他的眼睛因他经常使用眼药水而透露着微光。他目前正就读于哈佛大学（Harvard University），并在哈佛讽刺文社（Harvard Lampoon）担任艺术总监。他的成绩表现并不亮眼，也几乎不像一名学生。

结论

和许多首次货币公开发售(ICO)的产品不同之处在于，信用协议(CP)所能提供的不只是一个空泛的承诺 —它是一项可立即提供价值的实用协议，并且提供渠道以有助于用户广泛的采用，并可为代币买家带来重大的好处。其市场显著，用例也相当清晰，对其潜在开发者及用户几乎不构成进入门坎。它满足了以太坊生态系统中的缺陷，并可为未来的开发者提供一个可以实作创意想法的平台。CP兼具安全和新颖、勇于冒险和深思熟虑的特性。最重要的是，它 现在就能马上使用 。

更加令人兴奋的是， CP和FiD对于我们达成以太坊世界的愿景是客观必要的一项步骤。债务是经济成长的关键因素。若无债务移往区块链，加密货币生态系统就必然停滞。CP可促成下一阶段的以太坊发展。其中，大规模项目和基础设施的创造将难以和区块链分割。

CP的实作应用，可藉由纪录交易媒介、计价单位、储存价值和延期付款标准等方式让货币创造的过程更加自主化。事实上，由于个人无须拥有以太币就能在以太坊网络中提领以太币债务，因此我们完全可以想象未来被记录在CP上的债务和信贷可能超过所有加密货币的上市总值，从而显著地提升数字经济的规模。

同样地，Friend in Debt (FiD) 是一项专为未来需要而现在就已建构完成的应用。它可以确保全球形成一个去中心化的交易网络(decentralized transaction network)，赋予个人权力，并免除银行和Paypal等大型机构的繁文缛节和谋取暴利等问题。它相信个人的能力和群众的力量，从而让个别能动者得以掌握自己的金融命运，并鼓励各社群进行各类经济开发。

在BlockMason，我们相信以太坊的未来，但以太坊的未来需要信用协议(CP)—这个平台将可前所未有地吸引全球用户，并可实现以太坊的潜力，其不仅可为受欢迎的加密货币提供支持，更可产生相关应用的完整生态系统。以太坊的成功，也代表我们的成功。

咨询服务

BlockMason CP产品的专用代币买家，能根据一项产业标准授权协议，收到一个已完全缴清费用的永久授权，并可使用部分的CP网络容量(与买家购买的代币数量成正比)。Foundation、Credit Protocol、Friend in Debt和所有相关文件记录和支持结构的产权及所有权均归BlockMason所有。BlockMason有权调整每一个CPT所能取得的网络容量和交易次数，以在合理的努力中维护CP网络的运作效率和避免超量。我们针对产品专用代币进行首次货币公开发售(ICO)并非投资要约。买家购买首次货币公开发售(ICO)的产品专用代币时，应自行评估我们的产品和个别买家的既定用途及产品未来发展的可能性。我们提供的产品乃"按原样出售"的产品。买家可根据 beta测试版本和产品的文件记录自行判断。我们不对产品的适销性、特定用途的适用性和非侵权性提供任何保证。我们无法保证服务不会中断，也无法保证以太坊网络的质量。买家需自行查询产品适用的本国法规。

我们的法律顾问已发出法律意见书。其法律意见书表示， 美国的证券法规并无理由阻挠在美国的人士参与BlockMason的首次货币公开发售(ICO)。

Our Full Legal Opinion