eidoo

技术白皮书

版本0.2-草案-2017年9月21日

项目目标
用户体验
“智能”资产
交易所
身份
一个目标，两支团队

目录

项目目标 2
用户体验 3
“智能”资产 4
交易所 6
身份 7
一个目标，两支团队 8
Ethereum 团队 9
Ethereum：途径和方法 9
Ethereum：钱包架构 10
Ethereum：“智能”资产 12
Ethereum：交易所 13
Ethereum：身份 14
Ethereum：市场 15
比特币团队 16
比特币：途径和方法 16
比特币：钱包架构 17
比特币：“智能”资产 17
比特币：交易所 19
比特币：身份 20
比特币：市场 21

项目目标

过去数月乃至数年来，人们日益热衷于加密数字货币和所谓的“区块链技术”（来自比特币（Bitcoin)中引入的“区块链”数据结构，首次尝试解决分散式开放网络中的二次付费问题，并获得成功），这一现象目前已达到新高度。初创公司、财团和企业正不断推荐全新业务模式和应用程序。这套技术的众多建议用例已经超出无许可支付和价值贮藏等浅显易懂的应用领域，目前表现为严重的局限性、明显的缺陷性、盲目的预期以及不明确的目标。不过，有一类特殊应用程序显然正异军突起，足以引领市场新趋势：该应用程序将区块链技术用于发行、传输、存储和交换自定义的数字资产（即“代币”）。数字资产通常较具优势，不过在谈及区块链技术在管理方面的特定优势时，这一话题就较为庞杂，涉及对安全性、易用性、审查阻力、效率、隐私、可审核性、无许可创新和应急标准化等特点进行深入完整的权衡分析。优化这些权衡点固然雄心勃勃，却也困难重重，因为涉及到应用密码学、博弈论、分布式系统工程、开源式开发、用户体验分析、以及安全导向型电子产品等诸多学科。迄今为止，在向主流用户提供若干产品方面，目前在数量、完备性、资金供给和满意度方面均不尽人意。这些产品可用于平衡所有选择，尽可能发挥优势，以及最大限度提高易用性。

EIDOO 项目是首个具备开放性、包容性、全局性的项目，致力于打造高效的“区块链人机界面”，简化用户与基于区块链的资产之间的互动，同时保留这项技术的主要优势。其成果体现在：可提供一整套产品和服务，实现全新、直观、简单、一致和安全的用户体验，专注于以简单安全的方式存储、购买、出售、转让、交换基于区块链的数字资产，包括所有主要的“加密数字货币”和“代币”，以及用加密数字货币付款但不依赖任何中央机构购买或销售任何商品。

EIDOO Wallet是整个项目的核心所在。EIDOO Wallet将成为本地多元资产，专门针对移动世界（即单一的集成环境）而设计，将用于直观地管理所有代币，无需复杂配置，却仍可充分利用最佳安全标准和最佳惯例。交易所加密数字货币和代币的创新服务直接集中到平台中。这种集成化交换系统无需将资产转移到集中托管第三方（否则可能因漏洞、黑客攻击或退出骗局而造成财务损失）：用户始终完全掌控自己的资金。从长远来看，EIDOO路线图还包括一个基于区块链的完全分散式市场。围绕这些分散式工具将产生其他服务，从而有利于使用加密数字货币，例如，在不停止应用程序的情况下，能够通过EIDOO应用程序直接为借记卡充值。对于有需求的人士，EIDOO也提供数字身份解决方案，此类方案采用匿名主权身份信任网（Web of Trust)等设计，同时集成数字身份证。

EIDOO将成为增值集成商，将可靠的技术与现有服务、以及目前只能想像的其他服务整合到一起。EIDOO的目的不仅是“为人所不能为”，还包括使用更安全简单的方法重新考虑已完成的工作，重点关注用户体验，使其能够自由选择，同时令“加密世界”化繁为简、易于管理。我们意图建造一座通往世界的桥梁，而时至今日，距离目标还很遥远。我们的注意力集中在以下方面：向用户提供完整产品，使其直观安全地管理复杂事项。

这一项目还面临巨大挑战，那就是为技术社区提供共同的家园和共同的目标，这些技术社区支持不同愿景，从而导致办法、方法与设计理念间的良性竞争。区块链空间的权衡既困难又复杂：只会“妥协”通常造就两个领域最差者，而最佳选择有时是实现路径的多样化，在全球用户体验不变的前提下实现相同的最终目标。这也是一种风险管理策略：投资不依赖单一模式的项目，使我们能够减轻面临的技术风险，在金融和安全影响无处不在的创新行业中，这种技术风险非常之高。当今世界日新月异，优秀的解决方案止步不前就会被淘汰：作为一种方法对策，EIDOO将继续提升技术效率、安全性和用户体验。

用户体验

我们的任务是创建一个单独界面，与不同的技术堆栈和不同的设计理念进行安全互动，自始至终提供独一无二、始终如一而又不失简洁的用户体验。EIDOO 团队包括这一领域的顶级专家，他们与技术设计师悉心配合，携手完成这项任务。

当今的解决方案往往会走极端：一方面，一些工具既安全可靠，又易于使用、方便舒适，却只基于“极客专享”理念设计；另一方面，一些简简单单、华而不实、外表美观的产品又会误导用户，鼓励甚至推动不安全做法，令用户的金融资产面临风险。区块链相关项目使用一些术语和概念很常见，不用担心能否完全理解。虽然有些权衡本质上无法避免，但我们相信，科技先进和安全的最佳实践应有利于所有用户，而非仅仅“专家”，因为不负责任地使用技术往往会对他人造成负面影响，而且用户也应意识到，他们需要与所用工具建立信任关系。我们相信，有时需要*接受*未来工具在设计方面的内在复杂性：化繁为简往往不切实际。我们努力工作，帮助主流群体使用这些技术，同时也推动人们以负责任、可持续的方式谨慎使用这些技术。就分散式系统而言，管理数字资产的安全性，在传统金融领域的含义不尽相同：它需要用户更多关注、实践和意识。在“打造自己的银行”过程中，权力伴随着重大的责任。我们希望在设计以用户为本的解决方案时，能够以安全性、透明性和可理解性为出发点。

单独安全密码不受后台所使用的特定类型区块链平台、标准和技术堆栈的影响，且十分有利于跟踪和维护安全实践，即使对于不太擅长技术的用户也是如此。这是区块链技术安全模型的核心所在。与此同时，现有的易于保护平台接入点这一特色，不应将安全功能降级为模块化隐私保护功能、良好的熵产、易于移植、安全备份程序等。正因如此，我们才决定使用“分层确定性钱包(Hierarchical Deterministic Wallet)”方法让应用程序变得安全，因为该方法允许用户对其资产以及易于使用的过程拥有更多控制权。利用这一功能后，用户只需使用一个密码短语（可在12个普通单词中轻松编码），即可保障所有多元资产账户和地址及其签名密钥的安全。我们认为，承认和尊重他人的私有财产也意味着赋予其能力，让他们以其认为最佳的方式组织其私有财产。正因如此，我们才提供一种特殊工具，其无需中心服务器，允许用户在任何必要的地点检索和恢复数字资产。这款 EIDOO 恢复工具也被设计为让用户在紧急情况下需要代币时，能够以简单易行的方式充分使用代币。

人们往往根据以往经验评估服务质量，数字资产交易也不例外。对于数字资产来说，数字资产“钱包”的交易明细应一直易于阅读和导航，始终一致、内容详实、直观有序。我们设计出一种解决方案，可将处理和组织区块链系统中存储的信息所需的大部分复杂工作，根据具体情况从本地应用程序外包给服务器，而无需牺牲隐私性和安全性。钱包会自动检测到新型自定义代币，这些自定义代币可用于简单、安全的命名系统 (Naming System)，旨在避免钓鱼行为和欺诈活动。就精心设计的用户体验而言，对身份、声誉和地址的优化管理是其另一重要组成部分：EIDOO钱包专注于这一点，实现了安全最佳实践与使用舒适性的完美统一。

“智能”资产

Eidoo Wallet及其周边的所有产品和服务，将对基于区块链的数字“智能”资产的安全和简单管理作为中心焦点。

人们对数字资产兴趣日益浓厚，这在某种程度上表明这些资产可成为股票、债券、借据(IOU)、权利等的代用品。发行和转移资产的传统方式仍然缓慢、成本高昂、效率低下，而且从技术和监管的角度来看，也存在很多冲突。近年来，为了尝试利用区块链技术改善这种状况，我们已经做出一些努力。尽管有时真正原因可能与市场营销有关(由于“区块链”和“加密数字货币”的大肆宣传)，但我们认为，为了发行、存储和传输数字资产而结合或替代集中式信托系统，并出于这种理由使用区块链技术，这种行为本身就很有说服力。我们将开发 EIDOO Wallet，持续专注于

上述理由，最大限度发挥区块链相关的新工具和实践的优势，同时尽可能减少痛点、冗余、无用的过度设计和技术死胡同。

其中一个原因有时被称为开放数字资产协议的“社会可扩展性”：尽管集中式专有解决方案很难推进，但可以利用开放源码的实际标准来降低应用冲突，提高交互操作性。就区块链技术的内在价值主张而言，当某些市场定位中的区块链技术达到临界应用量时，数字资产也可发布在利用现有优势的同一平台上：钱包、市场、交易所、流动性提供者、图书馆、街区探险者、应用程序界面(API)、监管框架、安全硬件、用户习惯等。必要的自定义越少，过程中的冲突就越少。

另一个令人信服的理由是“模块机密性”：虽然基于信任的集中式解决方案会让用户面临隐私方面的问题，使发布者面临极大的监管负担（KYC、AML、隐私法、资产特定法规和授权等），但在技术上不可能的框架下，这些痛点可以得到缓和。

混合交换解决方案中的一部分数据在Eidoo云中维护，因此这些解决方案受常用KYC-AML实践的限制，而分散式解决方案将维护用户设备上的这些现有数据。

这一功能不但在隐私方面为用户提供了优势，也令数字平台日益受到关注，而且从监管角度来看，就发行商本身而言也免除了其责任。

使用基于区块链“智能”资产的第三个原因是“模块化可审核性”：虽然集中式、基于信任的解决方案允许发行人千方百计地修改分类账，例如，（鉴于某些条件）可以使用提高供应量、改变分布、黑名单总数和用户、更改交易历史、区块链技术，从而提供正确行为的可靠证明。通过正确的方式，可以使用区块链技术进行加密和独立审计，从而证明其发行的资产量、储备、总账记录的不可变性。

最后一个相关原因有可能实现“强力自动化”：交易对手风险极低（或没有）的无信任或最小化信任、自动和不可停止的契约，都可能成为基于区块链的资产的自然拓展。“红利”、“特许权使用费”投票权等广泛金融工具的自动化、全数字代理，对于现有的集中式混合用例已经令人关注，但对于更高级的场景可能最重要：基于预言的“智能契约”、“智能财产”、“数据访问对象(DAO)”等等。没有交易对手风险，十分有利于众多金融、商业和后勤用例的社会可扩展性。

交易所

加密数字货币的出现极大推动服务的分散化，使得用户基础更为透明安全，因为它避免单一故障点，并且人人都拥有完整的会计记录，可以看到所有正在发生的事情。基于信任的集中式交易所易于使用，提供先进的交易功能，但它们具有安全和审查风险。尽管一些交易所比其他交易所受到更好的保护，但在加密数字货币领域，黑客行为并不罕见。主要故障（从MtGox到最近黑客攻击）显示生态系统特殊点的极端脆弱性，不然就是极其强健甚至反脆弱。

可行解决方案可能是分散式的、不可靠的交易，不依赖于受信任的中央第三方来持有客户的资金。此场景中，通过自动化流程在用户之间直接交易。分散式交易所相对于集中式交易所具备以下优势：“无信任”（不需要相信交易所的安全性或诚实性）、公开审核、正常运行时间保证、隐私。

无论如何，这一想法都存在严重缺陷。目前的实验中，用户有时需要持续在线或执行复杂的操作，交易极其缓慢、成本高昂，流动性非常低，高级功能缺失。尽管一优势十分明显，但是目前纯粹去中心化的环境现在已经被一种情况破坏，那就是用户的操作效率已经比不上其集中式环境中的用户。对于交易所等服务而言，速度最重要，正因如此，顶级交易商才会争夺从光纤到交易所的最短线路。

身份

有一系列用途需要将地址与精确数字身份联系起来，例如：

- 与政府认可的身份相关联的地址，例如，在公共管理中出于特定目的纳税或接收代币，或者用于像非去中心化的加密数字货币交易所的KYC-AML。
- 可能需要具有一定程度声誉认证的地址，例如商店地址、通过信任网络机制予以保障的身份。

Eidoo 将使相关地址的数字身份清晰可见，从而在某种程度上降低隐私级别。是否使用缩减隐私地址的权利始终由用户掌控。

一个目标，两支团队

Eidoo是一个雄心勃勃的项目，涵盖两种不同的方法和执行方式。对于基于区块链的智能资产，将呈现一个简单而安全的钱包：

- 基于ERC20标准和EVM契约，以快速、易于使用、具有颠覆性、灵活性、特性丰富、成套可用的Ethereum执行方式，使用带有嵌入式代币系统提供开发资金
- 以一种安全的、可扩展的、长期面向隐私合规的比特币执行方式，基于新的资产协议RGB和非链可信计算，采用传统的非盈利开源融资方法

Ethereum团队

Ethereum：途径和方法

去年，Ethereum区块链获得大量关注，很多公司决定利用它来开发自身的项目，同时利用 Ethereum的“智能契约”提供的极度灵活性。

这导致Ethereum代币的增值，但与此同时，在承诺方面，用户应用程序在可用性和安全性级别方面尚未同步发展。

这样做是因为Ethereum是一种高度实验性技术，仍然不完善，而且在快速发展。此外，对于Ethereum所提供的智能契约，所启用的“基于账户”方法在其他方面非常薄弱，尤其是在隐私方面。

Eidoo的目标是使用当前执行的技术，尽可能为用户提供最佳体验，努力填补主要技术空白，同时追随和适应平台的发展。

Ethereum：钱包架构

轻客户端

在Ethereum，“轻客户端”一词指的是一种技术，即比特币环境下的SPV通讯者。

简言之，它具有“客户端”的能力，验证所有散列链，这些散列链在验证其他节点收到的信息时需要用到；并且只与它自身的Ethereum 地址相关，而不需要下载和验证整个区块链。

遗憾的是，Light Client Ethereum 的具体执行方式并不存在，它们都是实验性的，而且在移动设备上运行起来仍然过于繁重。

Eidoo 的目标是在移动设备上拥有Ethereum轻客户端，但同时，它将采用以下折中方案：

- 索引区块链数据的服务器
- 用户设备上的客户端从索引服务器获得与其相关的信息
- Ethereum的完整用户信任节点，它的客户端将检查从索引服务器接收到的数据，具体视情况而定

仅完整节点还不够，因为通过该节点，只能知道地址平衡情况。Ethereum完整节点不需要索引所有涉及地址的交易(甚至无需知道它的余额）；它不对代币数据进行索引，从这一角度来看，Ethereum完整节点是简单地执行代码（智能契约（smart contract）），可以修改区块链中处于记忆状态的一组通用数据。

索引服务器的任务是完成对区块链所有交易的高级分析，通过地址来索引运动情况，发现表示代币的运动情况，并对代币的运动情况进行索引。

这项活动过于繁重，无法直接在移动设备上完成。

助记种子

Ethereum使用比特币和很多其他区块链所使用的相同数字签名算法。比特币长期以来一直为密钥生成和存储的标准下定义：BIP32和BIP39。

这些标准会定义如何根据层级从单一种子中派生出许多秘钥；以及如何生成和使用一个助记词短语，来获取秘钥生成的种子。
Eidoo使用同样的助记词来为所有管理的钱包生成密钥。无论它们是Ethereum、Bitcoin还是其他区块链，其区别只会存在于衍生路径中。这意味着用户必须小心，不要只保存一个助记词。

多钱包

Ethereum是一个“基于账户”的区块链，这意味着Ethereum帐户有固定的地址；所有相关资产（埃特、代币、以及所有与它交互的智能契约）都是公开的、与这个地址相关，而且完全没有隐私可言。
遗憾的是，当前情况下，用户可以尝试实现最低隐私级别的唯一方法就是在多个钱包之间手动分配资产，同时十分小心，避免将它们混淆。
正因如此，Eidoo让用户有能力管理多个单独钱包才如此重要；这是通过从相同种子中生成适当密钥来完成的，为所有钱包只保存一个助记词，同时使用不同的BIP32派生路径。

交易历史

Ethereum区块链直接存储每个账户的状态。因此，若要了解某个地址的余额，没必要知道该地址相关的交易。为此，大多数流通中的钱包客户并未提供有关交易历史的信息（尤其是来自其他账户的埃特应收账款）。

从用户观点看，Ethereum或代币传输的年表是基本信息，几乎与余额一样重要。

更为复杂的是，当我们处在智能Ethereum契约的中间时（且所有代币都是智能契约），在区块链上移动资产和Ethereum交易的概念之间不再存在一对一对应关系。

Eidoo 客户端主要使用“索引”服务器来识别涉及其地址的事务，所有事务数据分析逻辑（例如，发现代币转移）也在客户机上复制，以便使用完整、可信的Ethereum节点来最终验证信息。

Ethereum：“智能”资产

Ethereum协议在区块链协议中引入编写能力，然后在全球范围内验证通用虚拟机的状态，这些虚拟机驻留在网络的各个节点上。这种设计考虑到区块链使用的通用性和灵活性，远远超出简单的价值转移。除了能够执行和验证智能契约状态之外，Ethereum区块链还可用于在本地创建和管理自定义资产。这些资产实际上是与知名标准（如ERC20）相一致的智能契约。

EIDOO Ethereum钱包完全支持ERC20代币技术。

目前还无法执行ERC20代币唯一的名称和符号：用户可以创建与其他已有标识相同的名称或符号的新代币。这一问题涉及如何简单安全地使用钱包：每个代币都有一个不同的Ethereum地址，但由于该地址是复杂的字母数字代码，难以读、写、记忆和比较，每个代币通常通过名称、缩写和图标符号予以识别。EIDOO Ethereum 钱包执行一个专用索引（special index），该索引将对由具有合法/或非正式的公司发布的代币（或合法代币）进行分组。对于具有特殊索引中相同名称/缩写符号的代币，EIDOO在其上贴有不可信标签，以避免诈骗、网络钓鱼行为和/或误解。

代币自动发现

在Ethereum区块链中存储的帐户的状态中，只能找到Ethereum余额，找不到代币。实际上，在 Ethereum 看来，这些代币和其他代币相同，都属于智能契约；这些代币的余额仍然处于代币智能契约的状态。因此，有必要让用户知道直接查询智能契约的某个特定代币的余额，因为无法提前知悉某个账户拥有哪些代币。

幸运的是，转移Ethereum代币Ethereum交易可以通过存储在区块链中的数据结构来识别，称为交易收据。

索引服务器为与特定地址相关的所有交易编制目录，包括代币转换。此交易列表商的Eidoo客户端也可推断出代币类型，查询代币智能契约，从而了解余额。

Token Sal引擎

所有 Ethereum Token Sale的参与机制均基于认购数据网站上的发布（实质上就是你可以将 ETH 发送到的地址）。遗憾的是，网站并不适合发布这些关键数据，因为网站不包含任何已发布数据的验证机制。

因此，Token Sale的认购数据发布系统是第一个攻击点，最近已被入侵数次。

可以使用PGP之类的数字签名工具，但对于那些最终忽视它们的用户来说，他们并不熟悉这些工具。

Eidoo 将针对认购数据为 Token Sale的组织者提供使用数字签名的安全分发服务。将此服务集成到钱包中使签名对用户完全透明，并且可通过简化的用户界面进行认购，因为所有参数都可以自动化。

Ethereum：交易所

EIDOO Ethereum钱包旨在集成一个安全、透明和部分分散式的资产交易所，该交易所通过Etherey智能合约建立，该合约可结算和完成交易。由于每个用户都在自己的智能合约钱包中存放用于交易的资金，因此有必要采取安全措施。传统的分散式交易存在迟缓和高成本现象，这将因使用链下的订货簿和服务器而有所改观。如此一来，最终用户将能感受到熟悉的传统交易体验，他们能够在其贸易平衡所允许的范围内创建尽可能多的订单，并且在Ethereum上的订单达成并执行之前，他们不会被收取任何费用。该架构并非仅限于提供链下订单创建的功能，还可代表用户清除订单，并直接将订单信息传送至Ethereum以便结算订单。该架构提供多重安全保障，因为所有不同部分（如前端和订单服务器）都会对订单是否有效和可执行进行会计检查，如订单通过这些检查，将被推送至Ethereum网络以待结算，接着订单将经过最后一轮不可更改的检查，如果通过该轮检查，交易即告完成。相较于具有中央订货簿的其他分散式交易所，这种混合系统的交易速度更快，但要求用户自己清除交易，从而产生其他问题，即多个用户甚至可能抢夺同一订单，且他们必须等待结果看看哪个用户能够优先。可以设计一个在Ethereum上运行的智能合约系统，将驻留在芯片上的密钥对用作加密数字货币余额（包括代币和Ether）的所有权密钥。接着将所有权密钥与由政府鉴定的数字身份关联起来。这样便可实现一些有意思的可选功能，如找回密钥（丢失或被盗的智能卡），或可更安全地验证接收地址（如将代币或Ether直接发送至已经过政府验证的身份）的交易。

该功能由EIDOO中央订货簿服务器来处理，因为它会自动清除和划去列表中的链上待结算订单，且使最终用户操作起来要快得多，有望起到提升集中交易效率的作用。

得益于对集中式代码执行过程的加密身份验证，EIDOO将为这种代码的正确执行提供有力保障：不可能对潜在订单匹配算法进行任何恶意更改。

此外，该架构提供至少三重账务处理和安全保障，不可更改的智能合约即为最终和最关键的保障。

Ethereum：**身份**

过去十年来，高收入国家政府试行和部署了公钥基础设施(PKI)，为公民提供数字身份，方便他们访问政府机构并提升访问效率。这些公钥基础设施通常工作原理是，为每个公民提供一张带芯片的个人智能卡。芯片包含一个密钥对：密钥对的私有部分可用于进行数字签名或向不同政府机构证明身份。政府保留密钥对的公开部分，并组织和管理 PKI 的认证机构。这些智能卡具有实体钱包所提供的安全保证，即密钥对的私有部分不可轻易剥离芯片。

Ethereum：市场

使用加密数字货币后，也可无需使用货物的贸易中介机构，从而节省用户和商家的交易费用。为推动该类贸易，我们也将开发一个分散式市场。

在这个市场里，用户可以自由开店并销售其工作成果。其商店里的商品将由自己的服务器托管，但需要 IPFS 协议的支持。(https://ipfs.io/)

开始时，就像交换服务一样，商店的搜索功能将由 EIDOO 的集中服务提供。

等到我们确保其足够稳定可靠时，我们会增加一个更分散的方式来执行搜索。我们很可能通过Kademlia网络（Kademlia-network）这一方式来实现此目的。

代币转移的所有密钥将由用户全权掌控。交易将通过使用智能合约或人力托管的方式来完成，每次均由买方和卖方协商一致后予以选择。

每次交易都会有反馈，并经由用户和商店签字。所有反馈都将在IPFS协议的支持下实现本地和在线存储。

有关在EIDOO上使用身份的建议将在该项目的这一部分发挥非常重要的作用，我们将会研究这些建议，以便找到更适合这种用例的建议。目前还有许多团队正在致力于对 Ethereum(雷电网络和等离子体 (Raiden Network and Plasma))和比特币开发Lightning Network（Lightning Network)技术。

我们正在密切关注其开发情况，随时准备好在普通用户能稳定使用该技术之时就对其进行集成。

比特币团队

比特币：途径和方法

EIDOO比特币钱包将最大限度体现在以下重要方面：社会扩展性、可审核性、自动化以及（特别是）机密性；我们认为这些方面从数字资产基于区块链的解决方案中获益最多。所有这一切均采用基于对抗思维的并以安全为导向的保守方法，尤其关注作为比特币运行原理的典型特征的链下技术可扩展性。

我们认为很难针对特定用例(如一般性资产分配)推出新的解决方案。相反，我们相信可以采用一种普遍使用且广受好评的解决方案，该解决方案不仅能利用其本身的基础设施，还能利用其生态系统，同时减少所需的定制项目，最大限度地降低风险以破坏向后兼容性，并提高其使用率。如此一来，该项目就很可能被采纳，也更容易被接受。

此外，利用经证实为不可变的、可通过审查、且较为安全的现有生态系统，可为发行人提供一个可靠、公平和可供证明的环境。由于这种环境的可靠和确定性质可供查验，发行人可采用加密的方式证明任何交易的公平性，而不需要任何集中式的基于信任的当事人。

我们也应慎重考虑交易对方风险，因为即使目前正在开发无托管、无阻碍的全自动合约，但这些合约距离实际商业应用仍很遥远。诸如自动化原子级交换以及“股利”或“回购”代理的解决方案已应用于一些集中式用例中，并可为分散式交易所、基于Oracle的智能合约、智能财产等为期货的前景构建模块。当然，这些前景基于以下假定：独立的区块链资产直接被用作抵押品。

此外，在上个月发挥关键作用的可扩展性概念也至关重要。能够处理大量交易是项目的基本要求之一，因为这种限制会妨碍该项目的发展机会。

Lightning Network(Lighting Network)提供一个顶级解决方案，不仅克服了这一问题，而且还改进了该项目的其他已讨论过的主要方面，如机密性。

而该项目所有方面中最重要的一直都是用户的机密性和隐私性。基于信任的解决方案和Ethereum ERC20对于发行人来说存在几个弊端，包括在跟踪、管理或调节交易方面可能存在一些技术上的不可能性。毫无疑问，非正式发行人将对此特别有兴趣，而对某些受管制的法人实体来说，这在法规和声誉方面可能具有更大风险。

比特币：钱包架构

EIDOO 比特币钱包将能够以安全和方便用户的方式管理比特币区块链中的一般资产。我们已选择根据比特币生态系统现有的最佳实践来构建钱包，以便提升安全保障级别，并提高互操作性和与现有解决方案和服务的兼容性。

该钱包有一个主要特征，就是从12/24个单词中生成决定性的密钥对，根据 BIP39 标准，这些单词被称为*种子*。这种设计选择乃出于安全考虑而作出。而其他替代方案，例如使用密码短语生成钱包(脑钱包(brainwallet))，由于其信息熵水平较低，因此不予考虑。低熵会让他们更容易成为资金盗窃的目标。最重要的是，为了提高安全性，在创建钱包期间，用户可如BIP38所述使用一个密码短语来对上述过程生成的私有密钥进行加密。

该钱包的另一个主要特征是，根据BIP32生成私有密钥和地址，从而形成分层确定性的密钥树结构。这样便无需使用过多密钥对，那样做会不方便、容易出错、并且可能发生故障。这一过程也可通过旨在规范树的创建的BIP43和BIP44中所描述的两个扩展方式予以改进。这一组件十分有利于确保与比特币生态系统中最好的钱包相兼容。

默认情况下使用最佳实践。实际上，由于机密性至关重要，所以每次需要新地址时（如情况有变），该钱包就会如上所述按照BIP32、BIP43和BIP44生成一个新地址，以避免再使用旧地址。

除了保密之外，主要关注点依然是尽可能利用比特币基础设施及其生态系统方面的能力。因此，该钱包的实现需要用到LibWally—— 一个跨平台和跨语言的程序库。该程序库包含一系列已通过测试的用于开发钱包的基元功能集。这将提升该项目的稳健性、安全性和快速发展。

比特币：**“智能”资产**

与RGB钱包相伴的另一个主要产品是RGB协议，旨在开发一种可进行普通资产交易的不同方法，同时优先考虑机密性以及与现有比特币生态系统的兼容性。

为实现所需的保密等级，我们开发了不同方法来为彩色资产添加标签，使其独立于其他所有现有的彩色币协议，同时也是让其他通过比特币区块链或其自身网络进行法庭分析的任何关联方无法辨别的协议。

实际上，我们的解决方案侧重于资产历史记录保密性。不同于现有的彩色货币协议，我们只使用输出地址来识别彩色交易并核对其完整性，而不处理使用顺序、填充顺序、或其他基于输出索引位置的任何版本。实现所需隐私等级的关键是，彩色交易不能被处理交易双方之外的人解密。

机密性并非我们力求实现的唯一优势：兼容性和（大部分当前协议都无法实现的）SPV 节点以及可由不同资产定义的费用（通过级高的隐私等级实现，除非代币持有者决定赎回资产）都是很重要的功能。这两点被认为可选，这意味着：首先，变更协议不会对协议本身有特别的影响；其次，这也让发行人能够完全掌控自身资产发行的过程。

扩展性是RGB协议的另一个关键因素。为此，我们将会着眼于实施Peter Todd提出的一个新概念，称为证明链(Proof Chain)。实际上只查看发行交易的资产历史记录还不够，因为存在二次付费的相关问题。为解决这一问题，实际解决方案会将机密性和扩展性进行交易。使用这一概念可让我们改善目前状况，具体做法是使用一次性印章承诺利用发行人开出一个一方当事人没有二次收费的（带有印章的）证明。

RGB 协议也会有自身的脚本语言，从而有可能让资产发行人创建若干功能，用于描述代币交易商须遵守的行为，但为了避免智能契约及未定义密码行为的不确定性，语言不会是图灵完备(Turing complete)的。

此外还存在一个验证系统，该系统与脚本语言直接结合，用于检查资产历史记录是否符合契约脚本中的规定。发行人最终会为每个 RGB 彩色币随附一份人类能够读懂的契约。该通知会明确说明资产持有人在最终交易交予发行人后赎回资产时享有哪些权利。这份契约将由发行人进行数字签名，盖上时间戳，移交到发行交易过程中，以此由每个用户向下一位客户传递，最后被保存起来。该契约应与必要的证据、数字签名、时间戳证明一同直接保存在RIDOO钱包里；这样EIDOO用户便可更容易地主张权利，并让发行方能够保证行为坦诚且有证可循。

RGB脚本语言将进行版本更新，且其原始版本将允许验证规则在二级市场用户间传递数字资产。后续版本不仅允许每次交易中的所有用户均正确转让数字资产，还考虑到允许资产最终赎回的更为复杂的情况。此类规定的示例可能包括已转让资产金额对应的费用，以及为了让资产最终可赎回所需要的每次交易附带的及发给资产发行人的区块高度。本保守型政策将从一开始就为资产转让赋予协议上的安全性及可用性，使得很容易引入需要额外测试及验证的额外特征，而不会破坏向后兼容性。

最后，为提升脚本表达效果，RGB 协议会充分利用硬件安全模组(Hardware Secure Module)。HSM 是防篡改的可信任计算装置，能够运行通用脚本，例如用来描述资产行为的脚本。HSM 服务器也允许在比特币区块链上随意执行更复杂的智能契约，但同时也为硬件提供信息，从非链网点取回可以触发智能契约的数据。实际上，RGB协议本身即可利用其区块链内部的数据——就像区块链上的任何其他转让协议一样——因此也能利用非常基本的数据，例如时间、费用或金额。当发行人希望对数字资产进行编程（以便在现实世界发生意外时才进行转让）时，需要"先知"来触发智能契约。这正是 HSM（一位可以提供受信任计算机环境的硬件先知）能提供服务的情况，可以为发行人及用户提供超出想象的使用案例。

使用该技术时，进行资产交易的发行人或交易商被迫遵守契约条款以及资产可转让性的不同条件，让发行人或交易商想作弊时只有一个选择，即打破HSM。即便如此，他们也无法窃取任何物品。因此EIDO 会为此提供数台HSM机，并将其安全保管好，可以向整个网络提供智能契约及先知服务。

比特币：交易所

发展分散式交易所时，将严重依赖Lightning Network (Lightning Network)。分散式交易所将使用户能够在更安全、成本更低、更保密的环境中转让普通资产或加密数字货币。

现有交易所的最大也最被低估的问题是，用户需要信任对方，让对方完全控制你自己的货物。即使是与通常可靠且值得信任的客户交易，交易对手风险也始终考虑在内，因为灾害事故常常就在背后。我们能够利用Lightning Network摆脱任何交易对手风险，因为交易用户无法通过任何方式进行欺骗。

另一个重大进步便是，由于利用非链交易，用户可以在点对点分散环境下享有更好的隐私保护。

特别值得一提的是，得益于一种称为非链交易的技术，Lightning会给费用成本和等待时间方面有很大提升，而这两方面正是比特币 2017 年以来的两大弱点。利用上述机制,我们得以创造一个几乎无需交易的市场，并使得确认时间减少 10 倍以上。

此外，Lightning Network也间接带来其他好处，即提高了安全性，也提升了隐私保护。实际上，Lightning交易默认自动进行，意味着如果交易不顺，你会收到退款。交易对方无法窃取你的款项，也无法不定期地对款项进行拦截。

钱包会为特定资产进行闪电渠道开户和管理，使用户能够完全控制配置参数。同时，钱包也会充分利用优秀的路径搜索算法，该算法负责根据时间、费率/成本、费用权衡为用户资产寻找最佳价格。

比特币：**身份**

近年来，为推动数字身份的发展进行了大量工作，数字身份是一组可让系统描述外部受理人身份的信息。

现有的已投产解决方案要么:

——包括集中式授权，集中式授权有几个缺陷，例如：单一故障点，易受审查、隐私保护不足，要么

——用户体验欠佳，导致客户做出不明智决定，影响安全性。例如 PGP 在 1991 年发生的事。PGP 是一个加密程序，提供加密隐私以及数据通信认证。

为此，我们将提供一个基于Christopher Allen杰作的解决方案。Christopher Allen研究的名义是“重启信任网(Web of Trust)”，研究所依据的概念是自我主权身份(self-sovereign identity)。

自我主权身份由之前的解决方案衍生而来，不依赖任何中心化机构，而是基于三个主要概念：用户控制、安全性、便携性，这些概念同时也是EIDOO项目的关键概念。

上述概念可根据智能签名(Smart Signature)及分散式公钥基础结构等项目进行扩展。前者是一个新系统，旨在改进有限的传统加密签名系统，具备定义验证条件及为其编程的能力。相反，后者描述了一种方法，旨在利用分散环境应对旧的公钥基础结构在可用性和安全性方面的若干挑战。

EIDOO会跟踪“重启信任网”的相关研究，以便在钱包中集成一种解决方案，使用户能够创建自己的个人数字身份。

比特币：市场

另一个功能是可通过利用Lightning Network创建的分散式市场。在这一市场，EIDOO用户可以通过分散的、可供查验的诚信方式，通过使用HSM或第三方托管系统（而非仅转移资产）进行通用商品和服务的交易。

该钱包将注意提取 Lightning Network原有的不友好功能，为最终用户提供更愉快的资产管理环境。

大部分规则既适用于分散式交易所也适用于分散式市场，因 Lightning Network 是两个系统共有的共同要素：避免交易对方存在的可能性。如此一来，在抑制恶意第三方的同时又增强了隐私性，并利用最新技术，如原子级交换交易甚至是跨链式的原子级交换交易，将令市场更具活跃性和竞争性,促成市场上低廉的即时交易，如果我们着眼于比特币在2017年期间在这两个特性方面的表现，这将是一个巨大的进步。

分散式市场与分散式交易所之间的区别在于有无托管人，托管人的任务是决定参与交易的双方中哪一方应得到这笔款项。托管人的角色基于其声誉，其应有动力担任中立的第三方，而不可转移资金或对其中一方参与者有不诚实的作为。

已经开展不同研究，其中一些已用于生产中，例如比特币，其他还只是概念而已，如离散对数合同；第一个有一些集中的要素决定哪一方正确，而第二个是一个盲目的、不可靠的第三方托管系统，其产出不受任何影响。由于我们正在使用 Lightning Network，所以这一盲目的、完全不可靠的第三方托管系统的实现尚未归档。

我们将研究其概要，看看生产就绪示例（如 Bisq 或 OpenBazaar）及该领域现有的最佳研究，以了解预言之间的不同权衡。