tbDEX流动性协议 v0.1

作者：@TBD54566975[1]

(译者：@wenjing)

简要：tbDEX是一个发现流动性与交换资产的协议，资产包括比特币、法币、或实体商品等，其中控制资产交换风险所需的社会信任度是个棘手难解的问题。tbDEX协议采用去中心化标识符（DID）和可验证凭证[2]（VC）技术来建立与现实世界一致的身份历史来源，为建立数字社会信任提供一个技术框架，从而支持资产间的去中心化交换网络。不管是看作交易的一个属性还是因交易产生的后果，此协议的设计都对交易的匿名性不表态。相反，它允许交易方之间自愿地为某交易协商建立各方可接受的最低条件，而且在不需要集中化的中介和信托经纪的条件下，为支持法币和加密币金融系统之间全面普遍的转进转出交换机制提供基础技术设施。这样的设施可以让每个用户更方便地使用加密资产和去中心化的金融服务。

引言

我们正处在一个金融系统的十字路口。无信任、去中心化网络的出现为未来的商业行为可以在不需金融中介机构的许可、参与、或借助于其功效的情况下顺利进行提供了可能性。

全球范围内还有17亿人没有银行服务，但这个群体里有2/3的人拥有手机可以帮助他们享用现代金融服务【1】。他们没有银行服务的原因各异，但常见的原因包括成本、风险、和缺乏基础设施。去中心化的无信任系统可创建一个新的世界赋予个人更多的权益：个人有参与金融支付的权力，既不需信用水平的证明，也不需付得起账户费，也不会因为支付方或接受方与中介机构之间价值观的差异而受审查或干预。在这个新的世界里，互联网是参与金融系统唯一需要的基础设施。

与传统金融服务相比，一个开放、去中心化的金融系统可以让所有人都能在全球各地安全地，以明显更低的成本，并且在更包容广泛的范围，相互交易做买卖。除了创建新的货币外，智能合约也能根本地重塑未来的金融基本设施的运作方式。

tbDEX协议就是起源于这个让每个人都能实现此未来理想的愿景。现在的比特币和其它加密货币还没有到普通人可以日常使用的水平。比如说，开你的第一个加密币户头通常涉及到经过某个集中的交易所，然后还有多步的资产交换，每步都有交易费，才能开始使用去中心化的金融服务。除了这些门户机构和相关费用，对大多数人来说，这中间的复杂性和无法理解的流程都是不可逾越的障碍。为克服这些缺陷也有其它一些重要工作在进展中，比如开发Lightning[3]协议，但是它们还是有很多不足之处，让普通人望而却步，无法从传统的法定货币支付跳到可以直接自然地进出去中心化金融系统。我们需要一座更便捷的通往未来的桥梁，tbDEX协议就是为这个目的设计的。

---

[1] 译者注：@TBD54566975是美国数字支付公司Square负责去中心化金融产品部门的推特账户。
[2] 译者注：本文把credential翻译为凭证以便与certificate（证书）区别。
[3] 译者注：https://lightning.network/

tbDEX协议的核心就是支持交易方之间在没有中心控制的情况下形成相互信任的网络，让参与者直接地交涉互相的信任度（或者依赖双方信任的第三方来为交易方做担保），并基于感知的风险和其它特殊要求为其交易定价。

基本概念

信任（Trust）

tbDEX协议对信任问题的解决方法与其它去中心化的交换协议不同，它不采用所谓的“无信任”模式，比如不可分割的原子交换。乍一看，这好像不是很优化，尤其考虑到我们的最终目标是要处理像比特币这样的“无信任”资产。但实际上任何与法币系统接口的界面都不可能是“无信任”的，靠法币的那一端必然会在金融监管之下。这意味着任何价值交换协议必须在根本上用其它的方法来治理信任，具体地说就是基于信誉。

tbDEX协议大量地借用（虽然不是全部）已经很完善的现用的处理去中心化信任的模式，比如互联网安全所用的公共密钥系统（PKI）。

本规范在去中心化标识符（DID）标准【2】之上建立一个信任模式，其中信任是通过各种各样的认证方来治理的，最终由使用系统的各人各方，与实现加密币钱夹的开发者，以及/或者他们各自的委托方来控制。

本协议本身不依靠一个联盟来控制参与许可或使用网络，也没有所谓的治理代币（governance token）。从最抽象的形式来看，这个协议是一个可伸展的消息传递协议，它有形成分布式信任关系的功能，这就是协议的核心要点。协议本身并不决定某个人的钱夹和某个参与的金融机构之间的最优信任关系应该是什么。

这层信任关系的性质永远不可能是普遍一致的：不同的管辖区有不同的法律和规章制度，不同的个人和不同的机构有不同程度的风险容忍度，它还受价格和其它激励因素的影响。如果我们在协议层独断地决定如何交涉信任问题，就必然要引进某种形式的联盟许可制，从而违反最大地去中心化的原则。

去中心化标识符（Decentralized Identifier, DIDs)

去中心化标识符（DID）是一种新的标识符，可以用来支持可认证的数字身份。一个DID可以代表任何主体，比如一个人、组织、东西、数据模型、抽象体、等等，它代表什么是由DID的控制者决定的。和常见的联邦标识符不同，DID的设计目的是要与任何集中式的登记注册表，身份提供商，和证书颁发机构脱钩。值得特别注意的是，虽然其它方可以用来协助索取某个DID的相关信息，但是DID的设计专门让DID的主人不需任何其它方的许可就可以证明其对该DID的控制。DID是一种统一资源标识符（URI），把一个DID的主体与一个DID文档相连，从而支持与该主体的可信交互。

与DID相连的DID文档是个元信息文件，含以下两个主要的数据元素：

1. DID主人可以用来证明其对该DID的控制的*密码材料*（即公共密钥和数字签名）

2. 可与DID拥有者接触并交换数据的地点的路由端点（比如：身份枢纽个人数据存储和转发节点）

DID方法可以用多种方式来实现，但典型的好方法（如ION[4]）包含以下基本属性：

- 该系统必须是开放的、公共的、而且无需许可。
- 该系统必须可以有效可靠地抵制审查并防止篡改。
- 该系统必须生成一个记录，它是高概率最终化的，而且即使在系统出现分割、节点有意隐瞒状态、和节点间串通等情形下，还可以独立地确定地得以检验。
- 该系统必须不依赖权力机构，被信任的第三方，或其它无法通过市场竞争机制替代的任何实体。

可验证凭证 （Verifiable Credentials, VCs）

凭证在我们日常生活中很常见：我们用驾驶执照来证明驾驶车辆的能力，用文凭来证明完成了学位。在商业场合，签名的收据可以证明支付，还有消费者对商品的评介，以及个人与非政府机构之间无数的陈述或声明等都可以泛意地理解为“凭证”。所有这些凭证在单独的应用，或应用平台，和其它单独的交互时都很有用，但是以前没有一个统一的标准化的方法来表达广义的数字凭证，以便在跨应用域、跨联盟边界、以及整个互联网普遍地使用。

可验证凭证（VC）标准提供了这样一个标准化的、在整个数字世界适用的、表述凭证的能力。其凭证密码学上可靠，又尊重隐私，同时是机器可验证的。如果VC构建方法上加上零知识证明（ZKProof）【3】的加密算法（如SNARK凭证）【4】，则更可以加强对隐私的保护与安全性，防止在披露数据之间做交叉连接，减少披露的数据量，在某些场合甚至可以完全不需暴露源数据。

身份数据存储和转发节点（身份枢纽 Identity Hub）

人、组织、设备和其它实体之间的数字化活动大多需要交换消息和数据。为了让这些实体能够交换为身份认证、应用程序、或服务流程所需的消息和数据，他们需要有一个界面来保存、搜索、和提取这些服务流程数据。身份枢纽就是一种数据存储和消息传递的机制，每个实体可以用这些身份枢纽来寻找与某个DID相关的公共数据和需要许可的私密数据。身份枢纽用网状数据库结构来构建，一个实体同时可以运营多个数据库，相互间同步其状态。这样的方式让拥有者可以保护、管理、与他人交易数据，而不需依赖实际数据存储地点，或某家服务商特定的设施、界面、或路由机制等。

身份枢纽采用语义编码的消息和数据接口，所以它的编程接口（API）是可推理的，使用其接口时，你只需要知道你想交换的数据的语义类型。在这个接口之上，通过在界面外部制定消息模版和处理指令，我们可以实现多种多样的交互与流程，从而形成一系列元协议。

[4] 译者注：https://github.com/decentralized-identity/ion

协议参与方

可验证凭证发行人（Issuers）

发行人是可验证凭证的起源。组织和个人（通过他们的电子钱夹）都可以是发行人。举例说，一个有信誉的金融机构一般已经在做KYC[5]检查，这个机构可以很快开始给他们的用户发KYC可验证凭证。一个电子钱夹（即个体）也可以给一家参与金融机构打评语，比如她也许是有过不好的服务经历，然后把评语共享到网络中，事实上成为一种可验证的信誉反馈。

对发行人来说，在给金融机构发评语凭证时收费可能是一种可行的激励机制。这些评语凭证可以帮助此机构加强在产业链下游的可信度与合法性。值得注意的是，一个验证人（包括一家金融机构、一个电子钱夹、或某个人）不需要为此与发行人特意建立直接的关系，却可以接收并验证他们发的凭证。验证人只需要依据对某凭证发行人的信保程度来决定是否可以依此做相关的商业决策。

电子钱夹（Wallets）

电子钱夹作为个人或组织的代理帮助实现与金融机构的交互。更具体地说，电子钱夹提供以下功能（但不只限于此）：

- 存储加密的可认证凭证
- 通过搜寻身份枢纽发现相关参与金融机构
- 接受、发行、出示可验证凭证（注：发行凭证需要其用户许可）
- 加数字签名
- 存放交易历史

依据tbDEX协议开发的电子钱夹可以大大简化在加密货币和法币之间移动资产的用户体验。个人与组织不再必须用法定货币在另外一个交易所先买好加密币，然后再把加密资产转到其电子钱夹。同样地，把加密资产转回成法币也便捷多了。

本协议在传统和去中心化金融系统之间提供直接的转入与转出机制，这样电子钱夹的用户体验就可以高度流线化了，意味着用户可以放心地使用自控电子钱夹而不需因为担心安全或因为是自运营系统就不能有方便的体验。

大规模投放后，相互竞争的金融机构将为他们用户提高电子钱夹的流动性与竞争性，包括更低的费用和更快的交易时间。

tbDEX协议不对电子钱夹强性制约其它具体的要求。钱夹的开发者可以为他们想要的用户体验自行设计相应的功能特性。比如，一个电子钱夹可以用先进的算法基于交易速度、成本或以往的记录来选择金融机构，也可以把这件事留给钱夹的主人。开发者即可选择为某类交易事先选

[5] 译者注：KYC（Know Your Customer）是美国金融管制法律的一个基本要求，即：金融机构必须在开账户和提供服务期间验证用户的真实合法身份等。其它国家与地区一般也有类似法律要求。

好哪些金融机构，也可在第一次交易前先执行搜索与评估流程并事先向搜索到的机构索取与验证相关凭证。当然，某个钱夹也可以把所有这些留给用户去处理。一般来说我们建议以下两点：

- 可移植性：个人或组织应该可以无缝地将所有的凭证移植到另一个钱夹。钱夹永远都不应该把个人的凭证视为己有，或据为己有。
- 用户同意为准：钱夹必须在向它方出示凭证前征求用户同意，并且把用户的优先选择保存以改进用户体验。

参与金融机构（Participating Financial Institutions, PFI）

参与金融机构是指在tbDEX协议网上提供金融流动性服务的金融机构。tbDEX是无需许可的，即任何PFI都可以在网络中运行一个节点，不需经由任何第三方的批准，包括任何个人、联盟、或组织。每家PFI都有一系列DID标识符和一系列VC凭证来确认其身份。PKI可以是金融技术公司、地方银行、大型银行机构、或其它金融机构，但不限这些例子。一家PKI必须可以参与处理法定货币的支付服务，而且可以用法币买进卖出加密币资产。理论上讲，PKI可以接受或支出现金或支票作为实现加密资产交易的机制，但在本白皮书里，我们只考虑在线的电子支付。

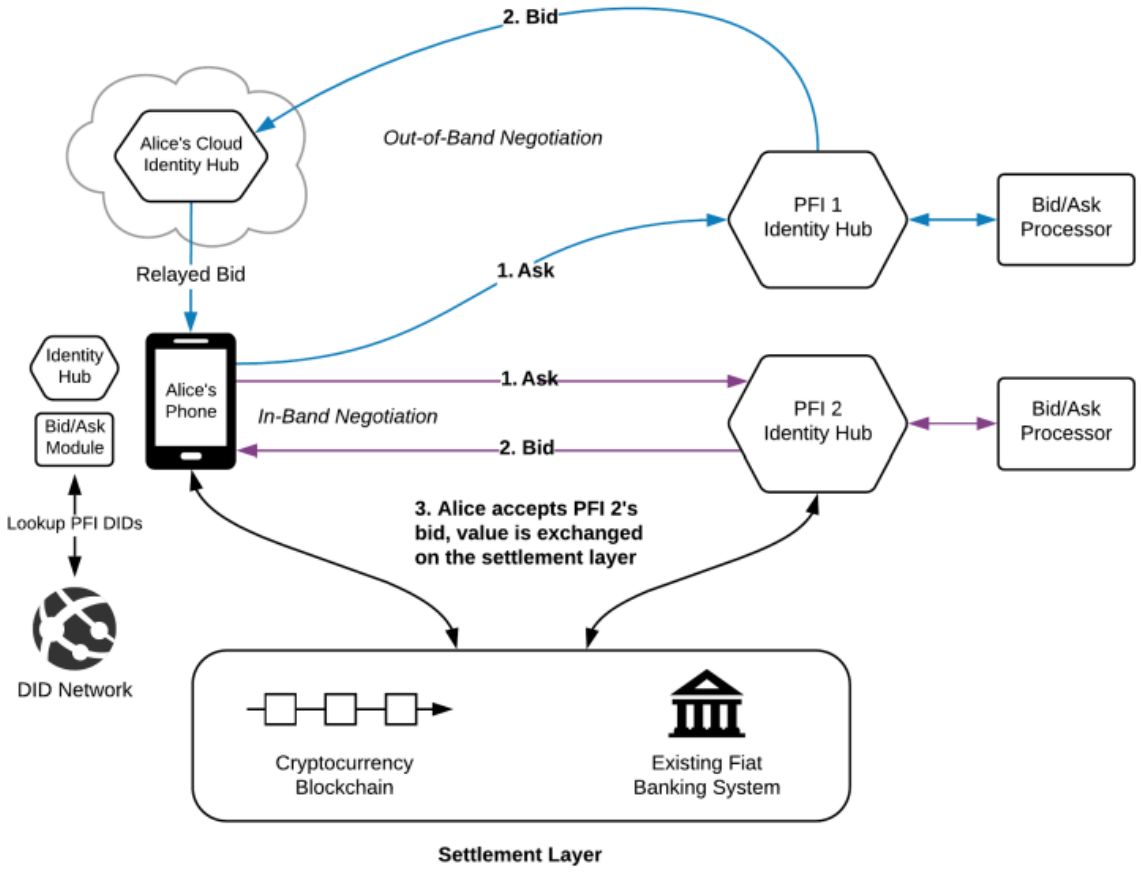
虽然PFI在不同的国家与地区会有不同的针对货币支付的监管规则，它们一般都需要向钱夹的拥有者收集个人身份信息（PII）以满足相关监管要求，比如反洗钱（AML）、反恐怖集资、以及不违反经济制裁等。tbDEX协议的问价（ASK）消息本身不包含PII信息，只是关于PII的类型，以及如果PFI接受此问价此钱夹会提供所需信息的承诺。

当一家PFI机构从一个钱夹收到问价（ASK）时，它根据ASK的详细信息决定是否返回一个出价（BID）。PFI不需支持所有可能的模版和ASK类型，比如，有些PFI接受信用卡，有些可能不接受。tbDEX协议消息里含PFI所需决定是否出价的信息，以及如果出价PFI需要向钱夹索取什么样的凭证。协议同时包含PFI为审查反洗钱（AML）和KYC所需的相关信息，检查通过后才向此钱夹发放流动性资产。具体的相关信息将依据不同地区的法规而定。

要参与tbDEX网络，PFI必须运营相应的节点来处理接受问价（ASK）与发送出价（BID）消息。概念上说，PKI的节点和钱夹雷同，也会使用同样的软件模块与代码库。tbDEX协议本身不执行纯法币或纯加密币的交易，这些功能由PFI机构来实现，用户可以通过此机构的DID标识符找到这些功能。

协议

核心的消息协议分为几个通讯协议层。第一层是个问价消息协议（Request For Quote，RFQ），某钱夹向PFI广播消息，寻找愿意与其用法币交换实物代币（稳定币或其它代币资产）的PFI，反过来的交易也一样。第二层的消息协议是个点对点的议价谈判协议，这个协议为钱夹和PFI之间提供安全保密的通讯渠道来交换所需信息达成交易价，并执行交易。



总体的模块级拓扑图和通讯流程图

点对点消息传递设计

钱夹拥有者和金融机构PFI之间交换的消息都会经过他们的身份枢纽，这些消息中包含了遵循标准模式的有清晰语意定义的数据体，这些数据体定义了实现问价/出价/结算所需的所有路径流程，还包含了交易方为评估请求、验证凭证、和执行交易所需的数据。

这些消息都是JSON对象，在每个信息交换路段由发送方签名送往接收方，根据其流程和内容需要也可以是加密的。根据针对各消息类型的语意和协议定义的规则，当这些消息到达身份枢纽时，其相应处理程序将通过提供的接口来处理这些信息。

发现参与金融机构

为了让电子钱夹能够发起与某些PFI金融机构做交易，它们必须首先知道这些PFI的DID标识符以将其包括在可用的交易方中。只有知道这些PFI的DID，电子钱夹才能得到交易方的现用公

钥以及与此DID相连的身份枢纽之路由端点。我们设想有几种方式可以让电子钱夹发现PFI的DID标识符：

个人采集的清单

个人可以自行采集他们想要与其交易的机构。电子钱夹设计时应该为此提供相关功能和用户界面让消费者可以简单容易地做这一步骤。

钱夹提供商采集的清单

最基本的方法是由电子钱夹的提供商编辑一个PFI的DID标识符清单，作为此钱夹的直接可交易方清单。钱夹提供商用他们的评估条件来决定选哪些PFI的DID标识符，例如验证PFI机构的相关凭证以及其它传统的商家与商家之间的认证程序。

对钱夹提供商清单的N-度爬虫采集编排

某个参与者可能从另外一方那里得到一个可信的DID清单，只需对这个清单里的DID按其自己的标准再做一个评估。这样消化了一个清单以后，该参与者又可以基于此清单里的DID，向这些DID索取下一层DID的建议。

DID目录爬虫

某些DID的实现可能提供对其DID目录空间列举的机制，如果这样，那么参与者可以对这样更广的DID空间爬虫，逐个询问其信任度凭证以及（或者）询问那些实体的身份枢纽所返回的可信DID清单。

最终还是由电子钱夹决定信任哪个DID清单和哪些PFI机构。

交易

技术假设

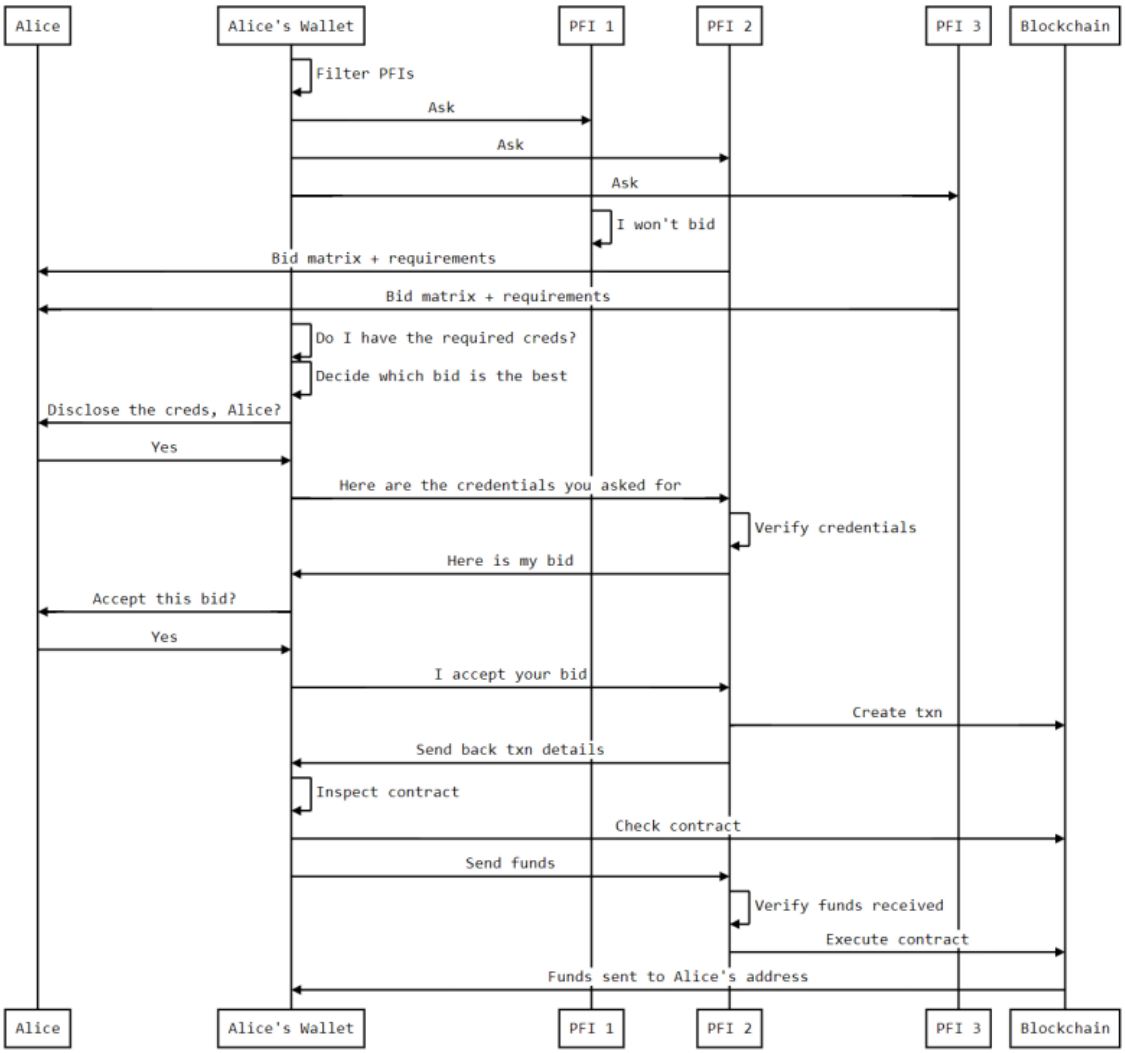
以下是此协议必要的前提条件：

- 电子钱夹的拥有者与参与的金融机构都拥有DID标识符。
- 电子钱夹的拥有者与参与的金融机构都有与其DID相连的身份枢纽。
- 电子钱夹的拥有者，通过他们的钱夹，能够经由采集的DID单子找到相关的PFI机构（包括钱夹生成的单子和/或动态爬虫发现产生的单子）。
- 电子钱夹的拥有者能够找到并获取PFI可能会要求的可认证凭证。

下面列举转入交易（即用法币买加密币）和转出交易（即卖加密币收法币）的例子，以爱丽丝（Alice）为例代表任何用此协议交易的个人。这个例子以美元为例，当然协议本身不限于美元。

转入交易例子

1. 爱丽丝的钱夹得到并缓存下已知和已发现的金融机构的公钥与身份枢纽之端点。这一步由电子钱夹按需定期执行。
2. 通过电子钱夹的界面，爱丽丝启动一个流程发出以100美元买入XYZ加密币的请求。
3. 电子钱夹产生一个代表爱丽丝的问价参数的语义消息（ASK）。
4. 电子钱夹发问价消息（ASK）给每个其选中为可行交易方的PFI机构的身份枢纽。
5. 感兴趣的PFI机构们对收到的ASK消息返回一系列的出价（BID）。注：*PFI可以选择针对哪个BID要求哪些凭证，甚至可以给一个不需凭证的BID。因为提供的可认证凭证越多，通常相应的风险越小，所以很可能PFI会对好价钱的BID或高速度的BIG要求更高程度的凭证*。
6. 爱丽丝从这些BID中选一个，返回该BID的散列（hash）的签名并出示所要求的所有凭证。
7. PFI验证爱丽丝所出示的所有凭证，如果一切查证成功，返回最终BID给爱丽丝。
8. 爱丽丝接受此BID，签名并送回给PFI。
9. 此PFI在区块链上发布一个智能合约，存入已由双方接受的数目的（即BID）XYZ加密币（以示其结账能力），然后把此交易地址寄给爱丽丝。
10. 爱丽丝的电子钱夹查询此合约以确认所示数目正确，然后从PFI的身份枢纽获取与其用法币（美元）支付的方法（展现为一些特定的线上支付服务）。爱丽丝从中选择她喜欢的支付方法，爱丽丝的电子钱夹则按所选方法的线上服务完成支付。
11. 一当此PFI对法币支付的状态满意了（这一步可以是等支付结账完成后，也可以早一些，只要此PFI愿意承担更多的风险），他们可以执行此智能合约将其加密币释放给爱丽丝的钱夹地址。

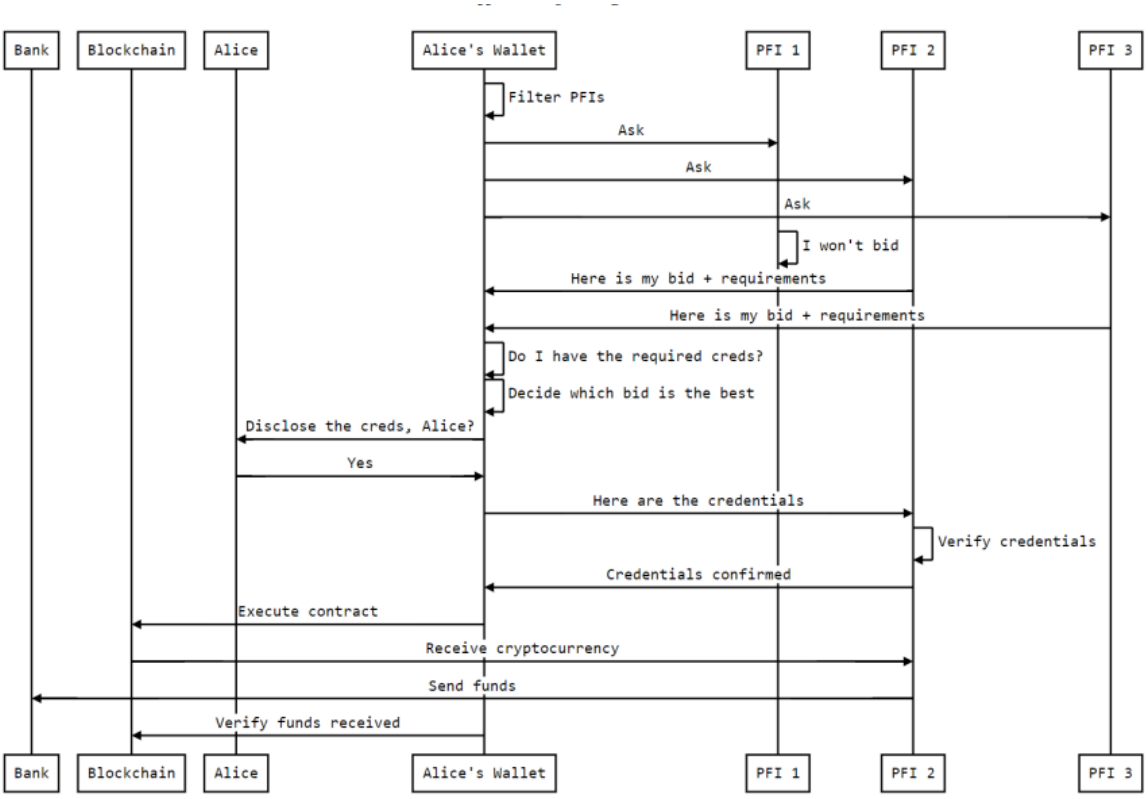


转入交易图示

转出交易例子

1. 爱丽丝的钱夹得到并缓存下已知和已发现的金融机构的公钥与身份枢纽之端点。这一步由电子钱夹按需定期执行。
2. 通过电子钱夹的界面，爱丽丝启动一个流程发卖出100枚XYZ加密币交换为美元的请求。
3. 电子钱夹产生一个代表爱丽丝的问价参数的语义消息（ASK）。
4. 电子钱夹发问价消息（ASK）给每个其选中为可行交易方的PFI机构的身份枢纽。
5. 感兴趣的PFI机构们对收到的ASK消息返回一系列的出价（BID）。
6. 爱丽丝从这些BID中选一个，返回该BID的散列的签名并出示所要求的所有凭证。
7. PFI验证爱丽丝所出示的所有凭证，如果一切查证成功，返回最终BID给爱丽丝。
8. 爱丽丝接受此BID，签名并送回给PFI。

9. 爱丽丝的电子钱夹在区块链上创建一个智能合约，存入100枚XYZ加密币，然后把此交易地址寄给此PFI。
10. PFI查询此合约以确认所示加密币数目正确，然后启动一个流程把法币资金转到其电子钱夹。
11. PFI将双方同意的法币数目推送到爱丽丝指定的目标。



转出交易示图

这里引入一个智能合约的目的是为了保证假如该PFI违约而没有兑现其合同义务的话，在智能合约中存放的加密币资产在过一段特定时间后会自动释放还给爱丽丝。

转出交易例子里的最后实际资产交换的两步对爱丽丝风险更高，因为PFI可以先提取爱丽丝的加密币然后把美元推送到爱丽丝指定的地点。理想的情况下应该要保证此PFI先付钱然后提取收到加密币。在以后的实现里，PFI和电子钱夹可以依靠某种银行的监控服务，作为智能合约里的预言机（Oracles）来监控此人的银行账户，从而确保只在它们看到法币支付已经启动后才释放加密币资产。

问价消息（ASK）属性

在上述例子中，发请求的电子钱夹发送一个问价消息（ASK）给PFI，其中包含评估此问价的关键信息。以下只是初略的解释以帮助理解，最终的协议定义会有些出入：

电子钱夹拥有人之DID

和该电子钱夹拥有人相连的去中心话标识符（可以是人或组织）

所请求资产类型

所请求的资产的类型（例如：TOKEN-USDC、TOKEN-BTC、TOKEN-MMXN、FIAT-USD、FIAT-EUR等等），其中TOKEN打头的是加密币，FIAT打头的是法币。

所请求结算机制

所请求的结算机制。这个属性让电子钱夹可以指定在哪个区块链或通过什么协议结算交易。例如许多区块链含有稳定币，而比特币可以像Lightning协议那样的以第二层的方案结算。对于法币结算形式应该包含比如SEPA[6]、ACH[7]、支付卡、SWIFT[8]或其它。

所提议资产类型

所提议的资产类型。类型与所请求的资产类型一样。

所提议结算机制

所提议的结算机制。类型与所请求的结算机制一样。

所提议资产数目

所提议的所要资产的数目。如果希望PFI来开个报价则可留为空白。

出价消息（BID）属性

从PFI发到电子钱夹的出价消息（BID）含描述交易提议的相关数据成分，包括报价、所需凭证和结算参数。

PFI之DID

与此PFI相连的DID。

提议的结算数目（符合ASK中所提议的资产类型）

以 ASK 消息中提供的资产类型计价的交易的提议成本。如果ASK中含"所提议资产数目"则该参数不需返回。

结算时限

结算将生效的最长结算时间（从出价被接受的时间算起）。如果时间超过则假定结算违约。

出价有效期

超过这个时间则出价被认为过期了，不再被PFI接受。

签名

[6] 译者注：SEPA: Single Euro Payment Area
[7] 译者注：ACH: Automated Clearing House 自动清算所
[8] 译者注：SWIFT: Society for Worldwide Interbank Financial Telecommunication

为了保证消息完整性用PFI私密钥在出价参数上产生的签名。

信任与信誉

电子钱夹和PFI金融机构之间直接协商以建立信任，也可以通过彼此信任的第三方为交易双方作保。tbDEX协议及其网络本身不为这样的可信第三方作特别的考虑，这一类的关系的建立与协议不直接相关，还是需要通过实际的人和人之间的程序还实现。

例如，某个电子钱夹开发者可以编辑并公布他们支持的PFI的DID清单，有些PFI会被排除在外，清单上也可以标明正面或负面的评语。这和现在的网页浏览器类似，它们预配置了可信的证书颁发机构（CA，Certificate Authority）清单，通过这个清单为TLS通讯建立信任基础以实现互联网上的安全数据传输。

对任何这一类的设计，有机制可以删除或修改某个DID在此清单中的信誉排名是值得建议的，这和证书颁发机构（CA）可吊销证书的做法类似。这个机制可以用可认证凭证（VC）并在身份枢纽公布的方法可靠地实现。这样一种方法的详细设计超出了本文的范围，但这是个重要的问题，我们将在协议运营化时予以解决。

风险和其它考虑

风险和针对PFI的考虑

受金融法规管制的PFI机构有一系列法律要求的责任，比如监控其平台防止洗钱或被恐怖分子和受金融制裁的实体所利用。除了监管责任和风险外，PFI们也必须管理金融风险，包括拒付、诈骗和违约。PFI的风险基本分三大类：金融犯罪、拒付/诈骗、承保/违约。

金融犯罪

金融机构对付这类风险的办法是建立一个牢固的反洗钱和反恐合规程序以监控非法行为。在加密币领域，许多金融机构采取了进一步的措施，利用区块链的监视能力和跨链分析方法以区分哪些人或电子钱夹可以与其交互，哪些交易可以执行。

与实现tbDEX协议一起，使用区块链数据分析和情报工具可以帮助PFI机构对个人的电子钱夹和交易进行筛选、评分、和监视，以便基于该PFI的风险规范和监管责任来评估交易。除了帮助检测与评估金融犯罪风险之外，区块链数据分析工具还可以用来基于以往交易历史估量风险级别，作为交易后的监察方法的一部分来检测之前遇到过的实体的风险。

拒付/诈骗

拒付（Chargeback）是指信用卡或借记卡的付款，在付款处理完结账后，由发卡银行把付款退回给持卡人。拒付发生在消费者因各种原因要求银行退还已付费用，最常见的原因是所购商品或服务没有交付到货，或支付卡未经授权使用。对tbDEX协议来说，拒付是一个额外的挑战，因为如果信用卡或借记卡用来购买加密币，而加密币存放到用户自己控制的电子钱夹之后，这份资产将无法取回。在这个例子里，用法币做的交易是可以逆转的，而加密币做的交易不可逆转

或退回。如何有效地控制诈骗和拒付风险是后面要克服的重要领域，本白皮书在未来版本会加以解决。

承保/违约

另外一个PFI需考虑的问题是电子钱夹主人在一项交易中答应要付的钱是不是所谓“好”[9]的。对世界不少银行系统来说，这是一个特别严重的问题，这些传统系统建立在老的基础支付系统之上，这些系统不能以“好钱”模式运营账户，不能确保余额不会变成负数。举例说，在美国处理支票的自动清算所（ACH）系统是个“发了就忘”的批处理系统，这些支票花好几个工作日清算是很正常的。在这中间的三到五个工作日期间，一些ACH的清算可以因多种原因被取消，包括资金不足、支票退回、账户关闭。不管是哪种原因，实际资金都没有到该收到的账号里。

对于由tbDEX协议处理的交易，只要账号的余额可能成为负数，PFI机构就有信用风险，因为承诺的资金会在交易结算前离开指定的账户。如果PFI出于加快交易速度以给用户近于实时的体验的目的，在ACH清算开始后但还未结账时就把稳定加密币送给用户的电子钱夹，那么这个风险会尤其的明显。

虽然银行和其他金融机构在传统金融中因此为潜在客户承保（并拒绝他们认为存在信用风险的客户），但还有其他发生违约的原因，包括交易本身在加密币已发送至自管钱夹之后失败。虽然PFI可以根据他们察觉到的违约或拒付风险调整出价（BID），这些情形值得在本白皮书的未来版本中予以考虑。

风险和针对电子钱夹的考虑

网络钓鱼

一个PFI 节点可以针对电子钱夹发起严重的潜在攻击，它可以伪装成合法的法币换入和换出节点，但真正目的是为了非法捕获个人身份信息 (PII) 或财务凭证以用于身份盗窃或财务盗窃。抵御这类攻击的第一道防线非常依赖于以相互共享的可认证凭证进行信任验证。因此我们强力推荐电子钱夹的开发者和运营者建立一个可信PFI节点的清单，并且这个清单必须可以被独立验证。否则电子钱夹的运营者在传输敏感信息之前须对交易方的可信度进行独立调查和验证。

结算违约/未交付资金

PFI在同意交易合约后，也可能因与诈骗或恶意无关的原因而未能付款。这也是个将在本白皮书的未来修订版中解决的领域。大致思路上讲，因为PFI的身份是认证了的，这为在技术之外用法律和其它途径解决争端创造了条件。这个问题也可以用另外一种解决方法，通过基于智能合约的托管结算（Escrow）或一种另外的瞭望塔[10]协议。

[9] 译者注：“好钱”（good money）一般指支付系统可确认支付方账户没有透支，收到的钱已完全结账，马上可用。

[10] 译者注：瞭望塔（watchtower）指一种在支付系统出现问题时提供保护服务的机制。比如：https://wiki.ion.radar.tech/tech/research/watchtowers。

关于匿名性和抗审查能力的注解

比特币白皮书【5】概述了一个无需依赖受信任第三方的数字原生货币和支付系统的愿景。 这是一个根本性的属性，它提供了抗审查、普及使用和安全等特性。

当电子领域和物理领域交接时，其无信任保障无法跨过这个分割线。虽然电子钱夹之间的比特币交易确实不需要可信第三方或中介，但在为商品和服务支付时，交易方的风险依然存在。在使用比特币时，收款人确实会收到资金，付款人确实不可能违约逃避金融责任，但收款人仍可能以不交付商品或服务的方式违约。一双物理的袜子不可能在交易所与比特币原子性地交换。其实，期望这样的交易可以完全匿名，没有与交易方存在某种外部的信任关系，这是不可能也是不合理的。一般情形下，收款人需要物理的送货地址，而付款人会寻找某种信号以确认收款人是个合法的生意。

法币与加密币之间的交换也存在同样的问题。你信得过交易方在收到加密币后会把法币付给你吗？如果他们不付账又能怎么样？

tbDEX 协议通过双方选择的第三方，利用去中心化的身份系统与可认证凭证来创建信任市场。这个设计也许会被认为是破坏了系统的匿名性，或非匿名化了交易，但是我们必须认识到，如上所述，商品和服务交易的匿名性是有代价的，即：无限制的交易方风险。

所以，我们的目标是抗审查、无需许可使用、和通过竞争达到最大流动性，最终在全球把支付普及商品化。我们的目标即不是不计代价地保持交易的匿名性，也不是夺走个人想要保持最高匿名度的能力。tbDEX网络原则上完全不排除为确保金融隐私的匿名交易。一家PFI机构原则上可以不要求任何可认证凭证，但这样做交易方风险会非常高。

待办事项

这份白皮书的初稿是为了帮助对提议的tbDEX协议高层设计的概念性理解，不应视其为完整的或最终的。它只是一个提议中的设计，以供公众评论反馈。

白皮书的未来修订版将解决其中不完整的因素和现阶段还未可知的问题与挑战。

在协议的设计最终被接受后，我们将制定并发布tbDEX协议的正式规范文本。然后下一步是开发电子钱夹的符合协议规范的开源参考实现和开发工具包（SDK），以及PFI节点软件的参考实现。

反馈

我们的目标是为了公共利益作为开源项目开发此系统。有很多事要做！实现tbDEX协议将面临无数挑战，有许多事我们知道还没有考虑到。我们欢迎您给我们输入如何改进这份白皮书。

任何反馈或意见，请发推文到：@TBD54566975，网址：https://twitter.com/TBD54566975，或在GitHub发pull request：https://github.com/TBDev-54566975/white-paper。

参考资料

[1] *The Global Findex Database* (2017), “Financial Inclusion on the Rise, But Gaps Remain, Global Findex Database Shows”; April 19, 2018 from The World Bank Group: https://www.worldbank.org/en/news/press-release/2018/04/19/financial-inclusion-on-the-ris e-but-gaps-remain-global-findex-database-shows and https://globalfindex.worldbank.org.

[2] *Decentralized Identifiers* (*v1.0*). Sporny, Longley, Sabadello, Reed, Steele, Allen; August 3, 2021 from World Wide Web Consortium (W3C): https://www.w3.org/TR/did-core.

[3] *Verifiable Credentials Data Model* (*v1.1*), “Expressing Verifiable Information on the Web”, Section 5.8 on Zero-Knowledge Proofs. Sporny, Noble, Longley, Burnett, Zundel; November 9, 2021 from World Wide Web Consortium (W3C): https://www.w3.org/TR/vc-data-model/#zero-knowledge-proofs.

[4] *Zero-Knowledge Credentials With Deferred Revocation Checks*. Chase, Ghosh, Setty, Buchner; July 13 2020 from Decentralized Identity Foundation (DIF): https://github.com/decentralized-identity/snark-credentials/blob/master/whitepaper.pdf

[5] *Bitcoin: A Peer-to-Peer Electronic Cash System*. Satoshi Nakamoto; (n.d.) from Bitcoin.org: https://bitcoin.org/bitcoin.pdf.