BLUE协议白皮书

2018年4月12日

摘要

Blue基于以太坊网络上提供一系列数字货币工具，例如开发者工具、客户软件和用户指南等。当前基础设施条件下，很大程度上依赖私钥和密钥的存储来验证资金的转移。这些都很容易被钓鱼、丢失或被盗，并且自以太坊网络诞生以来已经导致大量资金的流失。我们使用以下主要组件来保护用户资金、改善用户体验、确保数字资产的安全，并帮助以太坊网络和加密货币在总体上茁壮成长。

Blue 协议

一系列智能合约和后端系统使得所有网络在功能上更加安全和便捷。Blue协议允许在没有中间一方的情况下进行双因素身份验证。数字资产被应用于智能合同中，用户可以对这些钱包拥有完全的控制权。通过应用区块链识别系统、安全资产存储、智能合同分析、区块链分析、黑名单、白名单和防钓鱼能力，它们得到保护。

Blue SDK

我们为钱包开发人员、交易所和电子商务网站提供一种选择。通过使用Blue的钱包可以让让他们可以集成Blue协议到他们自己的系统中来让数字资产自动确认和自动转账。 通过集成易于使用的SDK，只需几行代码，我们的合作伙伴就能够展示他们对安全和保护用户数字资产的承诺。

Blue 钱包

Blue钱包是一个多平台应用程序，它允许发送、接收和存储基于以太坊的资产，如ERC20代币等。通过建立我们自己的钱包，我们就能够集成我们的安全协议。它包括分散式2FA，DAPP的深度集成，以及通过由区块链保护的互联网范围的标识系统下的用户友好体验。

Blue 标准

我们已经创建了一套开源指南，所以代币开发人员、ICO和其他数字资产创建者和基金托管人应该遵循这些准则。通过遵守这些准则和Blue协议，我们的钱包和SDK可以自动验证并且确保数字资产的安全。

目录

关于Blue

潜在信念

我们认为，去中心化加强了个人的隐私权和对其数据的控制。这对整个世界和全人类都是有益的。随着互联网技术的发展，政府和企业的监视也在增长。目前的市场状况，使得各组织可以通过监视和交易互联网用户的私人数据而获利。去中心化的资产是解决这个问题的第一个现实的解决方案。

我们认为，我们今天面临的阻碍加密货币和数字资产的最大问题是安全性差和复杂的用户体验。我们相信我在大部分人愿意并能够采用加密货币之前，缓解这两个问题是至关重要的。我们认为今天对于普通人来说，理解和使用去中心化软件是非常复杂的。大部分人不了解去中心化这个概念和去中心化的安全保障性质。

我们的使命

使密码更安全，更易于使用和理解，更易于开发。

我们的愿景

通过使密码更容易、更安全地使用，我们的目标是将密码货币和区块链技术引入主流受众中，使世界上的每个人都能参与去中心化革命。

当前市场评估

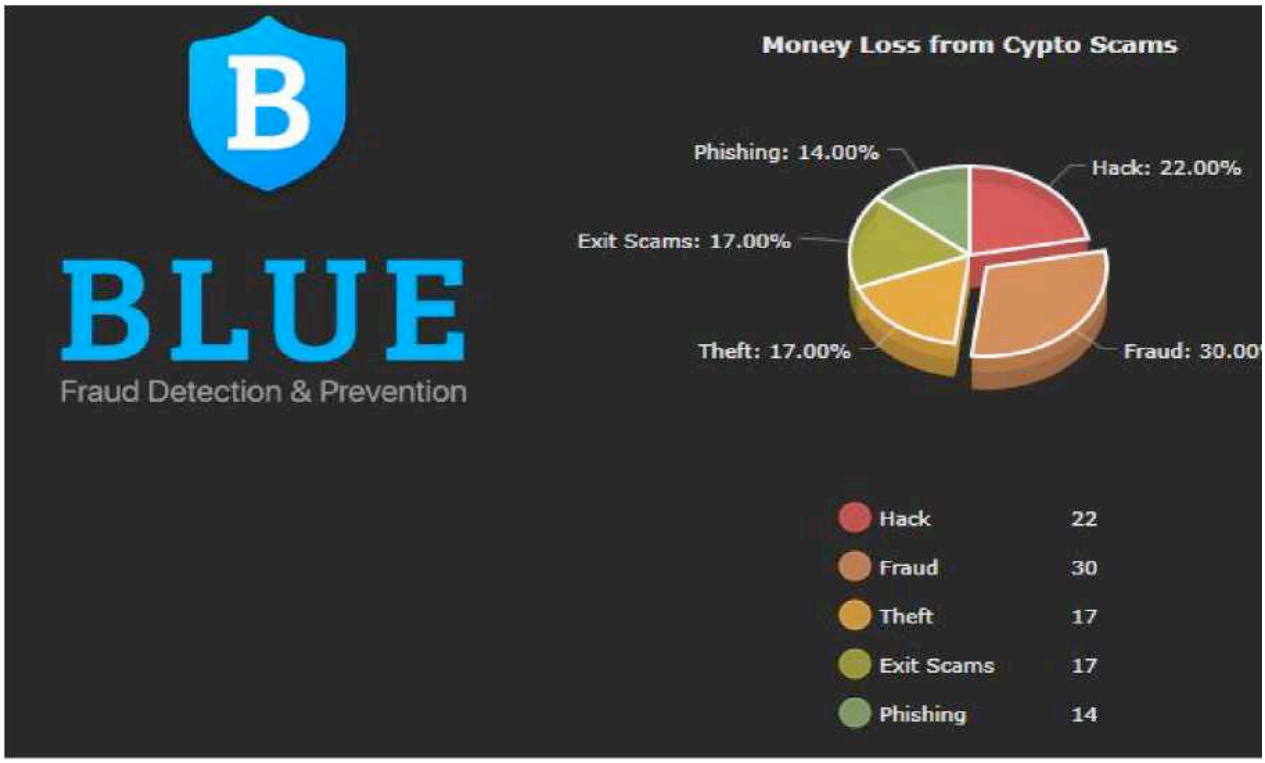
欺诈泛滥

在对100万份智能合同的分析中，一种名为MAIAN的新分析工具发现，34200份存在安全漏洞，在我们过渡到基于区块链的数字经济之前，我们需要解决这个系统的缺陷。（引用1）

引用1：https://arxiv.org/pdf/1802.06038.pdf

MAIAN标出了34200份合同，其中包括Parity区块链app的一个缺陷，该app在2017年7月使业主无法追回的以太币价值达到1.69亿美元。该团队随后手动分析了3759份合同，发现其中3686份合约中存在可利用的漏洞。这个应用程序使用了非常初级的工具，仅用智能合约代码的表面静态分析。 因此我们认为，34200份合约只是冰山一角。在我们对以太坊链上的Blue标准的早期测试中，我们可以确定事实是几乎所有的智能合同都至少有一个漏洞。根据我们的分析，近一半的智能合同都存在严重的缺陷。

2018年的头两个月里，超过13.6亿美元的加密货币因诈骗而丢失。在你读这句话的时间里，850美元已经丢失。（引用2）在2018年前3个月有超过22个独立的涉及损失40万美元或更多的案件。将这些损失加起来相当于每天1400多万美元(Kharpal)。



引用2：https://news.bitcoin.com/9-million-day-lost-cryptocurrency-scams/

ICO问题

在SatisGroup的SherwinDowlat&MichaelHodapp最近发表的一篇文章中，根据上述分类，我们发现大约81%的ICO是骗局，6%的失败，5%的已经消失。 有8%的继续在交易所交易(Dowlat)（引用3）。

ICO被分成几组，定义如下

1.欺诈(预交易)：任何表示ico投资的项目(通过网站发布、人工智能或社交媒体发布的合约地址）没有或者无意用资金履行项目开发职责，并且被社区（留言板，网站或者其他）认为是一个骗局。

2.失败(交易前)：成功筹集资金，但没有完成整个过程。因资金不足（未达到软顶）而被放弃，和退还投资者。

3.死亡(交易前)：完成融资过程，获得资金。币种没有能上交易所，并且从那时起三个月内没有在Github中贡献代码。

4.衰退(交易)：成功筹集资金并完成了这一过程，并在交易所上市，但仅有以下一个成功标准或者没有：

（1）部署(测试或者beta)链/分布式分类账(就基本层协议而言)或产品/平台(就应用程序/实用程序代币而言)，

（2）在其网站上发布了一个清晰的项目路线图，并且有提交Github代码。

（3）三个月内的代码贡献保持活跃。

5.有希望(交易)：上述两个成功标准。

6.成功(交易)：以上所有成功标准

代币让项目团队分心

因为大多数的ICO都是为了筹集资金而创建的，所以通常区块链技术并非实际需求。然而，这并不能阻止没有实际应用的ICO项目筹集数百万美元。这些钱来自不关心或者不知道如何评估技术细节的贡献者的资金。

引用3：https://medium.com/satis-group/ico-quality-development-trading-e4fef28df04f

这不可避免地导致项目团队专注于代币价格、交易和围绕代币方面的项目。这与发展过程相背离，对区块链技术的全面发展是一个整体的净负面影响。ICO团队通常只是炒作，而是不是落实在项目发展。这些通常以合作关系声明的形式出现，没有业务需求。忙于交易所上币，或者仅仅专注于故意操纵价格行为的营销活动。

缺乏效用

因为许多ICO项目只专注于使用代币来筹集资金，所以这些开发人员常常构建一个根本不起任何作用的代币，这对每个人都是不好的。因为没有实用利用价值，随着时间的推移，代币被初始购买者抛售。这些会导致人们失去兴奋感，而且往往会放弃这个项目。

故意诈骗

虽然我们上面列出的问题很可能存在于蓄意欺诈性的代币销售中，但是它们也可能存在于善意的开发团队中。这些因为缺乏知识或技能而导致最终退出。另一方面，如上文所示，81%的ICO是彻头彻尾的蓄意欺诈。这些项目对具有编程背景的投资人相对透明，因为技术细节经常剽窃，或无法使用，显然不是由一个有能力的开发团队创建的。然而，对ICO感兴趣的普通消费者很容易被愚弄。这是一个巨大的问题，并且是是对加密货币的头号威胁。欺诈性ICO的泛滥不仅制造了恐惧，赶走了贡献者人，而且还招来了政府介入并采取严厉的管制措施。

自我监管

自我监管是行业参与者自愿对行业活动施加限制和要求的行为。因为多年来，诈骗和黑客的数量持续增长，这在加密数字货币领域是必要的。如果我们作为一个行业不能采取行动提出我们自己的监管指导方针，世界各国政府将被迫介入，并有可能提出严苛的法规，这些可能会拖累该行业的创新和发展。人们更倾向于自我监管。现在是采取行动的时候了。这就是为什么我们引入了Blue标准，一个任何人都可以参与的开源指南库。

(Blue标准 https：//github.com/BlueCrypto/BlueStandard)

了解深入

与政府监管相比，提供自我监管的一个关键好处是，由于行业参与者对行业的了解，他们最适合提供这些指导方针和标准。熟练的业务，可以选择具有最积极影响的专家战略决策。如果交给政府监管机构，我们可能会发现加密货币可能会不再存在。因为机构对加密货币缺乏一定了解。

商业应用的更快途径

通过自我监管，我们就能更自信地谈论我们自己的产品，并给主流民众以平静的心态。这意味着随着时间的推移，用户将增加，我们也加快了发展。随着这些规则变得更加清晰和易于解释，这些规则可以被开发者简单地采用，从而允许通过有意义的商业应用来扩展新的创新技术。

提高投资者信心

有了基本的保障措施来监管加密货币行业，新的或好奇的投资者就可以更有信心地进入这个领域。计算风险是一个关键的方面，需要考虑许多动态因素。即使有成熟的法规，这对投资者来说也是一项艰巨的任务。这就是为什么要消除担忧，并给投资者心灵的平静，行业才能得以发展。

政府支持

世界各国政府都呼吁在加密数字货币行业进行自我监管。据福布斯报道，“美国商品期货交易委员会(CFTC)高级专员，共和党人布莱恩表示，加密货币领域的运营商可以考虑采用自我监管标准和‘全行业’的最佳实践来监管这项新技术。当局和政府正在考虑采取进一步的管制行动”。（引用4）这一态度得到了无数其他人的赞同，并代表着对自我监管的积极展望。

引用4：https://www.forbes.com/sites/rogeraitken/2018/02/15/u-s-cftc-commissioner-says-cryptocurrency-exchang es-adopting-self-regulation-could-spur-standards/

解决方案

Blue协议

我们发明并开创了一种模块化的智能合约系统。用户将元数据分配给他们控制的智能合约，允许代理控件、标识、2FA等。通过将这些兼容的智能合约指向另一个智能合约或一系列智能合约，开发者能够做出令人惊奇的事情。我们的平台将通过我们的框架和指南向开发人员开放。这打开了一种前所未有的方式来看待货币、钱包和货币的效用，这一切都是去中心化的。通过使用此协议和Blue标准，可以很容易地执行规则。 通过扫描代币、评估欺诈方和强制执行我们达成一致的行业标准，可以轻松实施自我监管行为。.

提升安全性

通过我们的协议，我们能够为链上交易创建安全的以太坊钱包。此外，通过遵循行业标准的安全要求，在传统的金融业界，我们开创了最安全的协议和应用。

改进用户体验

基于电子邮件的加密货币用户

用户只需知道他们的电子邮件，就可以发送加密货币给其他人。接收者将获得一条自动消息，允许他们通过下载一个易于使用的钱包来获取价值XX的XX个货币。这是一个类似与Paypal使用和发展的系统。它给我们机会来发展和市场营销。

基于智能合同的钱包

智能合约是在区块链上的可编程代码，它的地址，就像一个标准的以太坊钱包一样。在Blue，我们认为这提供了一个尚未开发的机会，可以做出惊人的事情。我们发明了一种方法，让每个人都可以轻松地为任何用户创建一个基于智能合约的钱包，然后像普通钱包一样继续使用它。我们避免过于复杂化的事情，在幕后不透明地发生安全所需地额外步骤，实现了无限的额外可能性和功能。在这里，我们将讨论Blue SDK在这个系统中将具有的功能的一些示例。

双因素认证

每一个网站和银行都需要这一点。 因为最终用户通常没有足够的安全性，所以我们需要更高的安全性。我们已经在区块链上建立了一个双因素认证系统。

以下是它的工作原理：

-用户制作智能合同钱包（1）

-用户选择双因素身份验证，这将创建另一个智能合约

-您的智能合约(1)指向双因素身份验证智能合约，要求它在交易上签字。才能继续下去。这可以由特定的总和，或者在任何时候，这也是由用户指定的。

-用户下载一个应用程序，为他提供两个因子代码，或者用户通过请求消息从受信任方获得两个因素代码。

-智能合约1查询智能合约2是否同意并通过交易

开支限制

支出限制是对用户进行的每一次转移的浮点数计算。他设定了他的转移限制或每单位时间的转移量(例如每天最多5个ETH)。智能合约跟踪交易，并触发任何用户想要的任何东西，类似于抛出操作。这也可以表示为安全升级，以便在继续之前请求双因素身份验证。

身份和收藏品管理

我们开创性的模块化钱包系统允许任何人向他们任何想要的人证明他们的身份，并且可以只用他们想要的身份的任何部分。

工作原理如下：

-用户键入他的秘密信息，他的秘密信息被哈希并存放在区块链上

-信得过的一方在这条信息上签名，说这是真实的

-这些数据现在以匿名形式存在于由受信任方验证的区块链上

-用户想要在某个地方注册提供证明他们的身份

-用户提交他们想要的身份的部分

-接收此消息的人通过与用户在其智能合约中具有的相同哈希进行散列

-查到说这些数据是真实的(如政府)

-我们现在可以信任用户的数据和身份

继承

我们的模块化智能合同系统将允许用户在他们的合同中添加可信方。这有效地允许用户选择各种钱包地址，这些地址可以将钱包中的所有资金都花掉。 我们也可以设定一个标准，其中只有在一定量的不活动或设定的时间范围内才是真的。

恢复

Blue将以继承的方式恢复代币和ETH。用户设置一段时间的不活动，并注册电子邮件或他们的首选被联系方式。如果这个时间通过，用户可以通过向Blue公司或使用我们的开放标准采用相同系统的任何其他提供者发送请求来触发恢复请求，Blue将收取一个小部分固定比例的资金用于回收资金的周转。如果两年不活动，用户将通过电子邮件提示。如果没有任何活动或响应，Blue将清空钱包，并按照现行准则没收。

自动结算所

自动结算所允许商家或其他供应商选择使用限额、退款机会，并且紧密的在多种类型的数字资产之间进行整合。

Blue SDK 定义

我们提供了一个SDK，允许第三方轻松地利用我们的系统和标准，而无需从头构建每个方面。这意味在以太坊网络上建立钱包、交易和其他运行，既可以大大提高其安全性，又可以节省开发时间。

开发人员使用以太坊进行的创新应该将他们的时间花在产品上并尝试新的东西。因为安全标准不存在，他们被迫转而专注于建立复杂的安全解决方案。我们的SDK允许这些开发人员与Blue协议集成，从而节省了他们宝贵的时间和精力，让他们能够专注于创新，同时保护客户资

金的安全。

因为Blue SDK是使用行业标准NPM打包构建的，所以它很容易跨多个平台使用。开发人员可以自由选择他们需要的方面和不需要的方面， 对于高度的定制和模块化来说是很有吸引力的。

Blue SDK支持双因素认证、防欺诈、安全资产存储、智能合约分析、区块链分析、地址黑名单、地址白名单和反钓鱼能力。

离链智能合同扫描

此外，我们的SDK还为消费者提供了请求对智能合约或钱包地址进行扫描的能力。通过使用我们的客户库之一来调用智能合约完成请求扫描。在队列中，扫描作业将由我们众多的扫描工作人员中的一个来完成。这些扫描工作人员可以进行横向缩放，以满足客户的需求。一旦扫描工作者获得一个作业，他们将针对智能合约的进行一些测试。这些测试的例子包括下面的内容。

集成测试

有关合同的副本部署到本地区块链。兼容测试是从我们的测试用例数据库中选择的，使用的是合约ABI，并且是针对智能合约运行的。

静态分析

使用许多不同的算法扫描智能合约的操作码以查找漏洞的模式。

黑名单和白名单

地址是对照一些社区和Blue维护的黑名单和白名单来识别已知的攻击者，并确认资金的接收者。扫描工作者完成测试后，结果被编译并寄存在我们的Blue服务器上。用户可以查看他们的结果，并获得对发现的每个漏洞的友好描述。

单点登录

SSO将允许用户使用一个单一身份来使用Dapp，网站和服务。标识平台包括详细的权限，所以用户可以分享他们想要分享的东西。政府机构、公司和其他机构将能够在我们的平台上为以太坊钱包提供身份支持。这是去中心化使用智能合约，允许任何团体提供身份来访问以太坊的消费者。例如，执行KYC的政府机构可能包括对以下领域的支持：

1.公共地址

2.用户名

3.实名

4.电子邮箱

5.政府ID哈希

这些身份可通过与发行机构，KYC或其他目前从以太坊生态系统中关键因素来验证。不能在没有发行机构私钥的情况下发现ID。这个系统的另一个用例是可收藏Dapp(如CryptoKitty)。它们可以提供有关可收集物品的数据，以便其他支持可以轻松地阅读和编写。真正去中心化的收藏品的模式。

SDK的案例

我们想要使加密货币更加安全和更友好的用户体验。选择SDK意味着当前的软件开发人员可以很容易地将其实现到他们的代码库中，从而提高安全性。这使得加密货币作为一个整体得到了加强，并加快了主流的采用。

我们的SDK还允许我们改变以太坊代币风气，这是我们所谓的“代币疯潮”。我们有大胆的设想，未来的用户可能需要6个不同的代币才能完成一次交易。这不是以太坊的如何来工作的问题，这种多代币方式将导致以太坊网络的减速，并降低用户友好性。我们通过我们的SDK和开发工具创作了一种全新的代币实用工具来避免这种情况。

Blue代币

Blue代币的用途非常简单。通过实时持有平台决定的一定数量的Blue，任何以太坊钱包都可以完全免费访问Blue协议功能。这适用于Blue钱包，任何使用Blue SDK的钱包，使用Blue SDK的交易，以及任何受支持的Dapp。代币可随时在二级市场买卖，用户可以使用代币获取Blue服务。如果用户决定停止使用它，可以很容易地将它转移到他们拥有的任何钱包中。无论是在支出方面还是在威胁分析方面，代币还具有独特的重放保护功能。Blue代币系统包含一个由nonce修改的加密签名和相关的元数据，因此威胁定义的更改不可能攻击代币的安全模型。

Blue代币的实际效用

由于几个原因，这需要一个代币。

首先，如果用户只需要持有ETH，就不可能免费为提供Blue成员服务。通过使用Blue代币来保证去中心化的服务，我们避免了每笔交易的费用结构，其中ETH需要花费在每笔交易上，或者在任何扫描以太坊地址的过程中。

第二，我们可以使用代币的智能合约来跟踪黑名单和白名单，并使用代币的智能合约中自定义元数据字段以及一个NONE来对黑名单和白名单进行跟踪和版本控制。这允许代币用于更改威胁签名事务的签名，以避免向网络广播虚假威胁签名。

第三，通过只向购买Blue代币的人提供服务，我们可以合理地让僵尸网络、垃圾邮件发送者和其他攻击者无法成功地发送垃圾邮件，以使其无效，或使其进程缓慢。对于攻击者来说，购买足够的代币来执行有效的Sybil攻击代价太高了。

Blue会员

我们希望为机构（例如交易所）的用户提供Blue协议功能，这在某些情况下是必须的。例如当交易所生成新的存款地址时，它会动态地处理此类经常变化的事物。在钱包之间不停地换代币会花费很大的gas。此外，大型交易所购买数百万个Blue从开放市场将对Blue的经济产生不稳定的影响。特别是如果停止使用，交易所就会将这些代币卖回市场。为了解决这个问题，我们创建了Blue成员制度。作为B2B客户的另一种选择，他们希望Blue代币的大规模部署。我们

提供了一个智能合同，客户的一定数量的以太坊地址在可以控制下的侧链下可以快速方便地使用。我们使用开发团队的代币，为这些功能提供动力，而无需到二级市场购买它们的代币。用户也可以直接购买Blue会员，而不是持有Blue代币和利用代币储备。会员采取固定的费用，是不可退款和不可转让的。

对于个人来说，最常用的方法是直接使用Blue代币。个人有更好的流动性与会员资格，并且从来不需要支付这些服务。我们将始终为Blue代币持有人提供免费的服务。

Blue钱包

Blue钱包是我们在钱包开发中的亮点，也是我们技术的展示。我们预计会有几十个钱包支持SDK的钱包，并以我们自己的方式来提高基于以太坊的加密货币的安全性和易用性。这个钱包，我们已经创建了一个演示，是最好的经验之一，可用于代币使用。我能够提供这种精简的体验，因为我们重视安全，这也使我们能够提供极大的便利。在未来，所有使用我们技术的钱包都会更安全更容易使用。

多平台支撑

今天，我们的演示钱包可以作为Chrome扩展，但是在接下来的一年里，我们将发布支持iOS、Android、Windows、MacOS和Linux的更新版本。每个钱包我使用我们的SDK来为我们的用户提供安全和方便，无论他们喜欢在哪里处理他们的业务。

DAPP支持

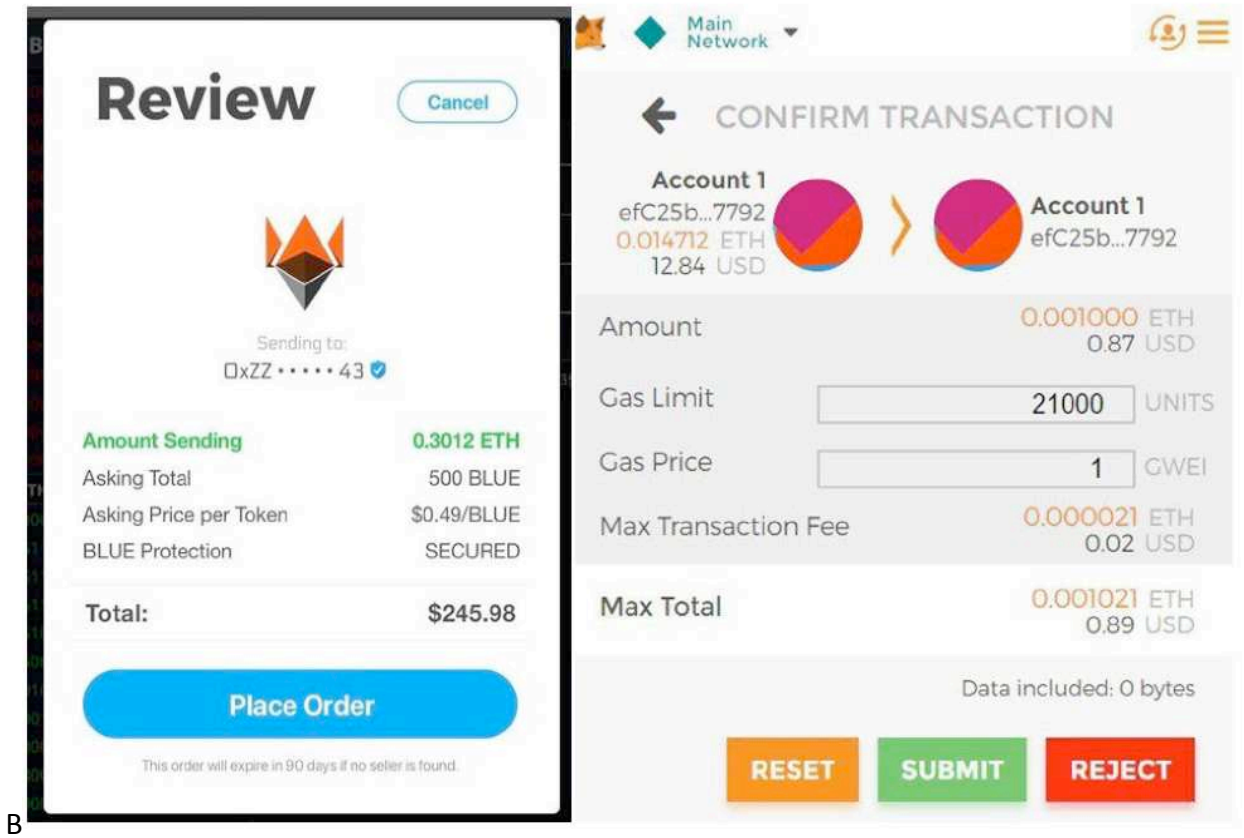
今天以太坊网络的一个常见用途是为Dapp提供网络，即去中心化应用程序。今天流行的Dapp包括EtherDelta、IDEX和CryptoKitty，仅举几个例子。通过将web3实例注入到用户的浏览器，我们提供了一个接口，这些Dapp使用您安全存储的钱包信息。这意味着你可以在以太坊网络上上交易，也可以在安全的环境下用Blue钱包来买卖你的CryptoKitty。

因为事务很容易使用基本的web3调用来代表您执行，所以简单地使用您的私钥登录是一个安全问题。MetaMask通过拦截技术部分解决了这个问题，这些调用并在允许它们通过之前

提供一个身份验证提示。目前由MetaMask提供的界面，钓鱼仍然是相当容易的。为此我们用一个叫做Dee dApp集成功能的特性来解决了这个问题。

深度dApp集成

通过与世界上最流行的dApp集成，我们能够在验证Dapp中的事务时显示用户友好的对话框提示。我们还使用徽标显示和验证的复选标记来唯一标记您正在使用的智能合约。如果使用Blue钱包，你将永远不会再被一个假的dApp钓鱼。如果这听起来很复杂，请参阅下图。将Blue deep integration与ForkDelta进行比较，而不是今天MetaMash如何呈现相同的信息。



Deep dApp 与 ForkDelta集成

2FA的必须性

目前，保护以太坊钱包的最佳方法是购买硬件钱包。这是因为私钥用在用于区块链交互的计算机外部的钱包上，并且密钥永远不会暴露给正在使用的计算机。没有硬件钱包，第二个最

佳选择是使用加密的签名-Blue钱包。但是，当此私钥存储在用户的计算机上时，很容易失去对它的访问权限，或者被网络钓鱼，恶意软件或者社交工程程序窃取。如果恢复助记词丢失，则可能会窃取硬件钱包的私钥。通过简单的恢复到具有相同助记词的另一个硬件钱包，很容易导致硬件钱包上的资金被窃取。通过提供双因素身份验证，即使丢失私钥也不会被盗窃，因为没有小偷会有身份验证代码。这比硬件钱包更安全，并且对加密数字行业的发展非常有必要。

中心化的2FA

目前，许多交易所和平台提供2FA，但这是集中的方式。这不能与分散的2FA混淆。双因素认证通常通过确认来操作。该密钥与身份验证设备(例如智能手机应用程序)和验证登录的集中管理机构共享。当交换被黑客入侵或数据库被入侵时暴露后，攻击者可能会窃取此密钥，用户的资金也可能丢失。更令人忧虑的是，交易所经常会失去自己的资金，而这些资金正是用户的存储资金。当这种情况发生时，往往没有任何追索权。这些集中的权力机构接受用户资金的保管，而你的余额只有在你信任他们将被控制的情况下才能真正得到，因为您相信他们会准确以一种欠条的形式保持你的正确的余额。区块链不能很好的保证这一点，并且在这些资金丢失时对整个加密行业构成持续威胁。当这些资金丢失。简单地执行2FA在中心化交易所并不能保护数字资产，而只用于保护您的帐户信息到交易所。

我们的解决方案

Blue团队设计了一个改进的HOTP算法版本，用于支持以太坊区块链上的2FA。通过将对代码注入的支持委托给智能合约(元钱包)，我们将允许支持2FA的第三方供应商。提供商使用Blue HOTP代码的开放标准。任何开发人员或团队都可以实现自己的版本并与自己的身份验证系统集成。这允许2FA不依赖于我们的服务。但是，为了方便起见，我们将提供自己的服务支持。

使用2FA代码的人应该非常熟悉这样的系统。在发送资金时，用户将被提示向钱包提供HOTP代码，然后才能发送资金。这些代码可以从兼容的智能手机应用程序中检索，这些应用程序可以生成一次代码。

这是通过我们使用的元钱包，一个智能合同和代理的用户存储资金，不是在用户的钱包，而是在智能合约。智能合约有效地实现了多重签名要求，所有者的私钥和第二个密钥都需要代

表用户对事务进行身份验证和处理。因为关键的恢复过程 对于每个事务的更改，攻击者不能使用相同的代码进行第二次后续事务处理。

一个本地移动Blue授权应用程序将被开发基于我们的改进算法产生HOTP代码。此算法是开源的，这意味着任何开发人员都可以使用相同的方案来实现一个相互竞争的应用程序或软件。为了方便起见，Blue的授权应用程序将被提供，并增加了Blue的工程工作的安全性。

区块链分析

Blue Geth是我们用GO编程语言编写的修改的以太坊节点。BGETH节点负责充分利用节点的数据价值，并对ERC20、ERC223和以太坊传输进行区块链分析，以此来识别有缺陷的合同、不良参与者和网络钓鱼。

通过直接集成，我们就能够扩展以太坊RPC API，并添加对代币、地址、转移和余额等评估。该系统简化了对节点的访问，执行速度要快得多。我们不是通过REST调用访问节点，而是直接访问数据，并在聚合REST调用中显示聚合信息。这大大简化了应用程序之间的工作量，从而减少了延迟、带宽和往返时间限制。

模糊测试

Blue的geth服务器允许我们对智能合同进行模糊分析，因此即使没有人工检查，我们也能够识别出有问题的合同。这使我们能够检测到代币可能会产生的情况。我们支持锁定转移，冻结资产，未经所有者批准转移资金，销毁资金，无限造币等等。

市场操纵检测

通过完全兼容以太坊网络，我们可以识别主要交易所的伪造交易量，计算任何代币上的真实流动性，检测交易所上的抽吸和转储行为，并发出警告。 此活动的用户。使用此方法，我们可以警告用户数量和交易价格的飙升，并通知他们寻找价格变动是否合法的证据。这适用于所有的ERC20和ERC223代币。

关于代币分布的区块链分析

在从ICO或二级市场购买代币时，重要的是能够获得分配公平性的一般感觉。如果代币开发人员仍然控制50%或更多的代币，他们很容易卖出大量的商品，给价格带来了很大的下行压力。在这个领域中经常出现这种情况，而且到目前为止，普通用户还没有确定这一特定风险因素所需要的工具。Blue协议帮助简化了操作，并且钱包紧密贴切用户体验。

许多代币开发人员持有他们自己供应的相当一部分。如果数量高于某一阈值，我们可以检测并通知用户。利用我们的BGETH系统，我们可以轻松地重组这些分析。

1.分析前10个钱包

2.确定真正的循环供应。

3.发现最高钱包之间的交易，这通常会是一种刷交易的形式。

4.检测开发人员的钱包是否被冻结。

5.分析前10位钱包，并确定代币分配是否健康。

Blue标准

Blue评估所有ERC20标志参加Blue认证程序的标准，这一格式受到以太坊EIP贡献者标准的高度启发。

Blue改进建议(BIPs)描述了在分配Blue生态系统中的声誉时，我们持有代币、钱包、交易所和其他区块链参与者的标准。

Blue标准是一个社区驱动的标准，将适用于每一个ICO和区块链为重点的公司/代币。让坏的项目可以被追查，给好的项目提供一种期望。我们期待他们提供一份“要做”的清单。例如，请参见下面的“Blue标准”中的无限造币项目。

Blue标准：无限造币

摘要

代币创建者可以选择让自己或其他人拥有造币的能力。我们认为这应该在时间、范围或数量上受到限制。无论是有意的还是无意的，我们应该在EVM中引入一个模糊测试层，它可以尝试随机输入，直到通过智能合约交互确定总供应量可以增加或减少为止。

动机

目前，普通投资者还没有明确的途径去知道一个代币可能会增加或减少它的供给。投资者理解的唯一途径是阅读和理解他们所提交的每一个项目的源代码。这不仅对技术熟练的投资者来说耗时，对新手投资者来说也是不可能的。从而出现了大量的盲目交易，投资者不知道他们的代币是否有固定的供给，或者固定利率的波动供给的支持。

实施细节

简单地尝试随机输入参数，然后计算总供应量以测量是否有任何一组输入改变总量。如果是这样的话，作为标准元数据输出的问题，我们将它作为布尔标志包含在Blue Geth中的TokenMeta.json中。

Blue标准的其他例子包括：

1.代币锁定

2.明确现金流量标准

3.创始人代币锁定

4.清晰的Howey结果

5.清晰的代币经济学

6.分别关注代币和ICO代码

7.代码标准-明确的功能描述，让投资者知道他们是否容易被欺骗。事后没有借口

8.ICO标准-为什么你的ICO需要一个代币？为什么它需要在区块链，并做出解释。

9.代码标准-gas使用。无用函数和依赖关系

10.命名约定的dApp标准

11.可接受的操作定义(数学方程式等)

12.禁止开关，除非有条件多重化

Blue协议的集成

钱包供应商的集成

钱包提供商将能够使用我们的SDK，并与我们的工具一起工作，使我们的许多功能在合作伙伴钱包中启动，例如

1.2FA

2.黑名单

3.白名单

4.代币分析

交易所整合

交易所将能够使用我们的SDK，并与我们的工具一起工作，使我们在合作伙伴交换中的许多特性成为可能。共同用途可包括：

1.2FA

2.实际交易量计算

3.泵警告

4.代币分析

5.黑名单

6.市值计算

7.开发团队持有量计算

区块链查看的集成和价格图表

区块链查看常见特性包括：

1.实际交易量计算

2.识别不良代币

3.实际流动性

4.代币评级

带头加密数字行业自我治理

今天Blue是唯一一个积极寻求解决自我治理问题的团队。正如我们在前面指出的，这是重要的，而且必须实现的。黑客攻击、资金损失、监管失败以及其他原因每天都会导致这个行业出现问题。目前主流上还没有采用加密货币，所以我们需要一个标准，并且需要行业伙伴加强自我监管工作。这就是我们所需要带进这个令人兴奋的行业的使命。

给监管者的话

加密货币世界比监管者更了解加密货币，更适合自我监管。考虑到密码的复杂性和独特的需求，自我监管的努力将成有助于保护加密货币投资者，同时不牺牲区块链技术带来的技术飞跃。如果世界各国政府希望继续管制密码货币，他们将会遇到越来越多的阻力。例如使用现在工作来掩盖加密交易和社区的反击。密码学是无处不在的，也是不可打破的。这些工具对世界是很重要的，而且我们必须保护那些选择与他们合作的人的权利。我们敦促监管机构让这个新兴的密码社区进行自我完善，并自我监管。