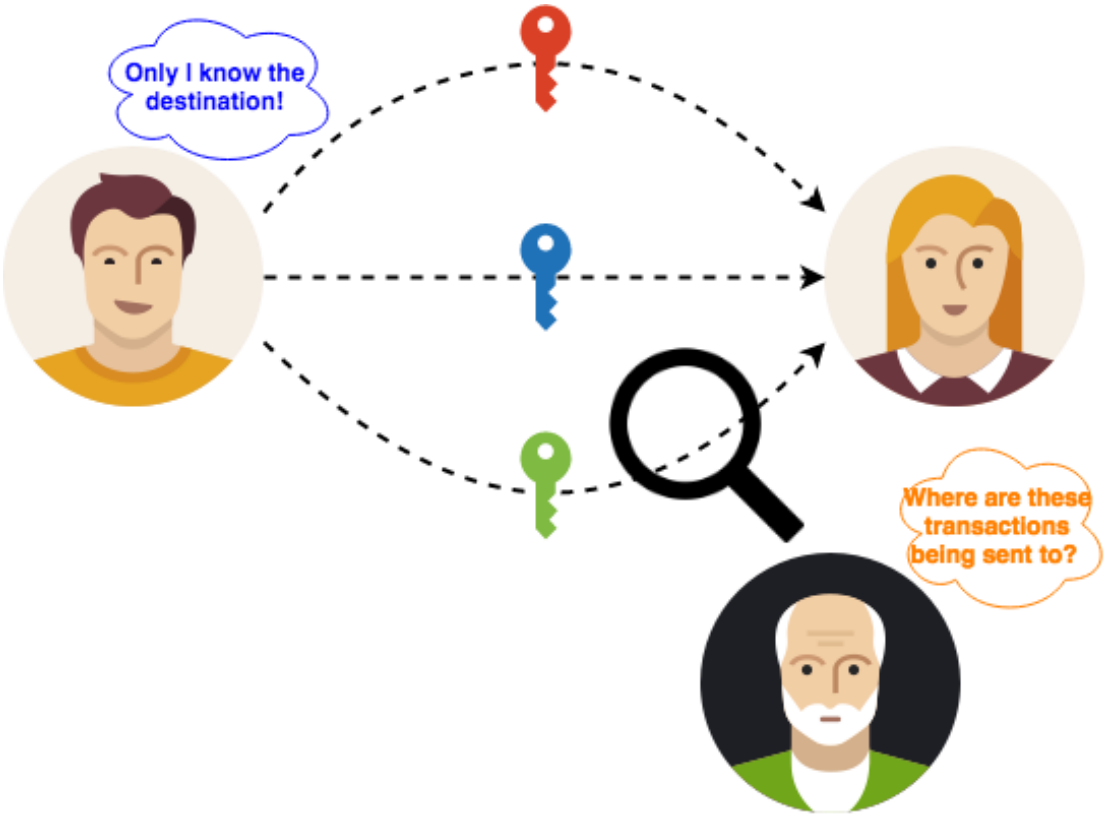
区块链隐私增强技术 — 隐身地址

今天的许多区块链，包括比特币和以太坊，都是公开的公共分类账，因为对参与者没有限制，所有交易细节都可以在区块链上看到。在公共分类帐中，交易实体仅由其从相应公钥派生的区块链地址标识。公共分类账一般被认为是 "伪匿名"，这意味着地址与一个人有关，但公众不知道该人。然而，通过分析交易图并与其他信息相结合，可以揭示区块链地址背后的真实身份，最近的研究也表明了这一点。由于各种原因，包括但不限于管理与执法有关的问题和隐藏敏感的、针对具体公司的信息，人们和公司更愿意在区块链交易中增加加强隐私的特征。

隐身地址密钥管理机制

隐身地址是一种隐私增强技术，用于保护加密货币接收者的隐私。隐身地址要求发件人代表收件人为每笔交易创建随机的一次性地址，以便无法建立向同一收款人支付的不同款项之间的联系。



基本隐身地址协议（BSAP)

最基本的隐身地址计划最初由比特币论坛成员命名为 "ByteCoin"，并在 2011 年开发的，该协议依靠椭圆曲线 Diffie-Hellman (ECDH) 协议，其工作方式如下:

- 发送方和接收方分别有私有/公钥对 (a, A) 和 (b, B)，其中 A = a·G 和 B = b·G 和 G 是椭圆曲线群的基点。
- 发送方和接收方都可以使用 ECDH: c = H (a·b·G) = H (a ·B) = H (b·A)，其中 H (·) 是一个加密哈希函数。
- 发件人只是使用 c·G 作为发送付款的临时目标地址。
- 接收方主动监控区块链,并检查是否已将某些交易发送到声称的目标地址 c·G. 如果有，则可使用相应的私钥 c 使用付款。

BSAP 的设计有两个主要问题:

i) 临时目标地址是在两个通信实体之间固定的。因此，这些实体之间的交易可以很容易地联系起来;

ii) 发送方和接收方都可以计算私钥 c。因此，如果收款人没有及时使用付款，发信人可以改变主意，收回钱。

改进的隐身地址协议（ISAP)

为了解决 BSAP 中的设计缺陷, Nicolas van Saberhagen 在 2013 年的白皮书中详细介绍了一个名为 ISAP 的改进计划，后者后来由 Peter Todd 在 2014 年的比特币协议中进行了修改。ISAP 是 BSAP 的扩展，它应用了如下所述的加法密钥派生技术:

- 接收器有一个私有/公钥对(b, B)，其中 B = b·G 和 G 是椭圆曲线群的基点。
- 发送方生成一个临时密钥对(r, R)，其中 R = r·G 并将其与交易一起传输。
- 发送方和接收方都可以使用 ECDH: c = H(r·b·G) = H(r·B) = H(b·R)，其中 H (·)是一个加密哈希函数。
- 发件人使用 c ·G + B 作为发送付款的临时目标地址。
- 接收方主动监控区块链，并检查是否已将某些交易发送到声称的目标地址 c·G + B。如果是，则可以使用相应的私钥 c + b 使用付款，请注意，临时私钥 c + b 只能由接收方计算。

虽然 ISAP 修复了上述 BSAP 的设计缺陷，但区块链节点仍需要使用其私有支出密钥 b 来主

动扫描区块链，以获取所谓的目标地址 c·G + B，这与安全存储私钥的常见做法相反。私人支出钥匙的持续使用大大增加了其被泄露的风险。

双键隐身地址协议（DKSAP)

为了消除 ISAP 的私人支出密钥过度使用的限制，DKSAP 是由一个名为 Rynomster/sdcoin 的开发人员在 2014 年为 ShadowSend 创建的一个双键增强，这是一个高效且分散的匿名钱包解决方案。自那时以来，DKSAP 已在一些加密货币系统中实施，其中包括 Monero、Samourai Wallet 和 TokenPay。该协议利用两对加密密钥，即"扫描密钥"对和"花费密钥"对，并计算每个事务的一次性付款地址，详情如下:

- 接收方有两个私钥对(s, S)和(b, B)，其中 S = s ·G 和 B = b·G 分别是"扫描公钥"和"花费公钥"。这里 G 是椭圆曲线群的基点。

- 发送方生成一个临时密钥对(r, R)，其中 R = r·G 并将其与交易一起传输。

- 发送方和接收方都可以使用 ECDH: c = H (r·s·G) = H (r·S) = H (s·R)，其中 H (·)是一个加密哈希函数。

- 发件人使用 c ·G + B 作为发送付款的临时目标地址。

- 接收方主动监控区块链，并检查是否已将某些交易发送到声称的目标地址 c·G + B. 根据钱包是否加密，接收者可以通过两种不同的方式计算相同的目标地址，即 c·G + B = (c + b) ·G. 如果有匹配项，则可以使用相应的私钥 c + b 使用付款. 请注意，临时私钥 c + b 只能由接收方计算。

在 DKSAP 中，如果系统中存在审核员或代理服务器，则接收方可以与审计代理服务器共享"扫描私钥" 和 "花费公钥" B，以便这些实体可以代表接收方扫描区块链事务。但是，他们无法计算临时私钥 c + b 并花费付款。

基于区块链的物联网（IoT）系统面临的挑战

DKSAP 为交易接收方提供了强大的匿名性，并使他们能够在实践中获得无法关联的付款。但是，这种方法确实需要区块链节点不断计算来产生和匹配目标地址，并在区块链中找到相应的匹配项。虽然此过程适用于成熟的计算机，但它给资源受限的物联网设备带来了新的挑战。因此，问题是"我们能否通过做出某些权衡来使DKSAP适应基于区块链的物联网系统？此外，由于存在临时密钥，可以很容易地识别使用隐身地址的事务，从而导致一些隐私损失。因此，另一个问题是"在使用隐身地址时，我们能否减轻这种隐私损失，因为存在临时密钥？"