区块链隐私综述

谢倩

1 比特币的隐私问题

1.1 比特币的背景介绍

比特币（bitcoin）是一种去中心化电子加密货币，于 2008 年由中本聪（化名）发明创立[1]。比特币基于区块链（block chain）概念设计。区块链是由所有参与者共同维护的数据结构，存放着比特币交易的历史记录。每块数据（创世区块除外）均有指向上一块的指针，形成链式结构。比特币用户使用化名，也就是比特币地址进行交易。比特币地址用于接受和发送比特币，功能类似于银行账号，但无需实名认证。每个地址对应一对公私钥，只有拥有地址对应的私钥的人才能支配地址中的比特币余额。每次转账时，发送方用私钥签名生成一笔交易（transaction），指定接收方的地址作为输出，自己的地址和自己作为接收方时的交易作为输入。如果一笔交易的输出尚未被作为输入写进其他交易，则称为未花费的交易输出（unspent transaction output, UTXO），一个地址对应的所有 UTXO 将作为其余额，可以用于转账/支付。如果一笔交易的输出已经列为其他交易的输入，则无法再次被支付，即不能“双花”（double spending）。比特币是公开系统，任何节点均可加入，通过工作量证明（proof of work）来促使参与节点达成共识，这相当于利用经济激励机制解决拜占庭一致性（Byzantine Consistency）问题：工作量证明需要参与节点积极诚实地记录每一笔转账，并给予激励。参与节点的计算能力越强，获得的激励（比特币）就越多。由于发行数量有限（总量约为 2100 万，平均每 10 分钟区块发行新的比特币，区块产生的比特币数量每四年减半），比特币可以对应真实世界的价值利益。因此参与节点为了获得更高的利益，会共同遵从共识协议的设计，保证一致性。

1.2 比特币的匿名性

比特币的匿名性本质是“去实名化”，即用户不用真实身份在网络中交易，而是以随机地址作为钱包，公钥哈希值作为交易标识，代表用户的身份，因此网络中记录的是一笔笔随机数地址之间的交易，无法将交易和用户身份联系起来。比特币用户就像披上了马甲，不能被轻易识别。然而化名不等同于匿名，匿名指的是具备无关联性，即攻击者无法将用户任意两次交互进行关联。但比特币中，或者其他基于区块链的数字加密货币都是以公钥哈希值作为地址进行交互，交易之间是存在联系的，所以比特币不具有匿名性。研究者就曾成功追踪了一名用户在 2011 年声称失窃的 25000 枚比特币[2],[3]。尽管追踪失窃数字货币看起来无害，但是相似的技巧可用于追踪敏感交易，从而侵犯用户隐私。

单个地址重复交易不能确保匿名性，那多个地址呢？同样也不行。即使用户创建多个新的钱包地址，但资金在钱包之间转移时也会连接起多笔交易，只要耐心追踪，还是可以将多个地址归属为同个用户，这叫“地址簇”。此外，由于比特币采用的是 UTXO 模型，每笔转账都是将“旧”的比特币花掉产生“新”的比特币，而且比特币交易是“多进多出”的，允许有多笔输入和多笔输出，这就有“零钱地址”的概念，用来将转账后剩余的比特币还给发送方。零钱地址也会暴露用户地址的关联性。早期比特币类库（Bitcoin-Qt Library）存在零钱地址总是出现在输出地址第一个的问题（2012 年修复）。将交易地址关联起来归并成地址簇后，攻击者再结合现实生活中的交易信息，如用户在交易所、钱包客户端等暴露的个人信息，给地址簇贴上认证标签，就可以解析用户完整的交易轨迹。此外，比特币支付不会传递身份信息，但使用者的 IP 地址是可查的。有论文[4]研究表明：捕捉网络层交易数据包传递

路径可一定程度上识别出交易来自于哪个 IP 地址，从而锁定交易的来源，也就查到交易者所在的位置，进一步破坏比特币的匿名性。

1.3 比特币的隐私建模与评价

比特币通过无需实名认证的地址提供了一定的匿名性。而且转账时，一个用户可以生成任意多的地址，并且使用匿名通信工具如洋葱路由网络（The Onion Router, Tor）进行网络连接，进一步实现隐私保护的目的。为了衡量比特币隐私保护的能力，一些隐私评价模型被提出，结合比特币交易去匿名化的手段，可以量化比特币的隐私性。

隐私评价模型的设计原则是充分利用已有的比特币交易历史记录和已知的部分事实，推断未知地址的真实身份，对比推断结果和真实结果，以及推断结果和随机猜测结果的差异，评价准确性。推断越准确，隐私保护能力越弱。

已有工作[5]设计了两种隐私评价模型：

1）地址可链接性推断，要求基于已知信息推断出两个地址是否属于同一个用户，该评价模型计算推断结果和真实数据的差异，以及随机结果和真实数据的差异，对比两种差异，作为地址可链接性指标。

2）用户配置不可区分性推断，要求对每个地址，推断出唯一的拥有者用户，该评价模型计算两种指标：标准化后的互信息（Normalized Mutual Information, NMI），用于评价推断结果和真实数据的差异；调整后的互信息（Adjusted Mutual Information, AMI），用于评价推断结果优于随机猜测的程度。此外，还可以计算推断结果中有多少用户的多少地址是准确的。

在进行推断时，主要使用两种去匿名化的技术手段：

1） 根据链上交易数据进行推断。最广为人知的是两类启发式规则：

- 多输入规则：同一交易的多个输入对应的地址属于同一个用户。此规则的原理是多输入交易需要输入多个地址对应的私钥，一般情况下只有用户拥有的多个地址会成为同一交易的多个输入。
- 影子地址规则：若一个交易中仅有一个首次出现的地址，则该地址和输入地址属于同一用户。此规则的原理是比特币客户端默认的“找零”行为会为转账/支付剩下的零钱创建一个新地址。

使用这两类规则可以在结果中不断扩大某用户拥有的地址范围。如果已知一些地址的真实身份，将有助于使用这两类规则更准确地进行推断，这使得刻意生成的新地址（甚至在 Zcash 等系统中使用零知识证明的私密交易）也会暴露真实身份。

同时，一个用户的转账行为存在着一定的模式。如果将某个地址的交易时间序列提取如转账金额，转账频率等特征，然后进行聚类分析，也可以提高推断的准确率。

也有工作通过结合超图(hypergraph)和交易模式来对特定类型地址，如交易所进行分类判别，从一定程度可以帮助确定身份[6]。

此外，对于洗钱等行为，还可以计算当前地址的资金“纯洁度”等指标，追溯资金源头，从而将当前地址和来源地址链接为同一用户[7]。

2） 根据网络通信数据进行推断，即利用比特币网络底层的转发规则，找出交易对应的 IP 地址，帮助找出比特币地址的真实位置[4]。不过此类方法对于使用匿名通信工具和非本地钱包的用户无效。

早至 2015 年的工作表明[8]，即使只用最基本的启发式聚类规则，一个用户有平均 68%的地址可以被成功地推断出来。在其他工作中，通过仿真实验得到的结果表明，超过 40%的用户的至少 80%的地址可以被找出来。

2 区块链的隐私保护

2.1 在比特币区块链基础上提高匿名性

2.1.1 基于不重复地址

比特币可以不受限制地创造新的钱包地址进行交易，为避免关联性分析，建议用户每次交易都用新的地址，所属地址间不交互，避免被归并到同一个地址簇。比特币每次交易会有零钱地址，所以尽量不要用零钱地址进行交易。目前比特币客户端 Bitcoin-core 默认钱包创建 2000 个地址供用户交易，也就是说每次交易的地址和零钱地址都不会重复，但地址数有限，当交易次数变多后就会重复使用，建议用户手动再创建新的钱包再交易。

2.1.2 基于混币方案

比特币交易记录会暴露交易关系，从而被追溯至交易源头，那如果交易路径足够长且混乱呢？这就会大大增加追踪的难度，混币方案就是以此思路保护用户隐私。混币（mixing/laundry）方案的思路为：将多个用户的交易资金混合在一起，通过多笔交易转移，最终分发到目标账户。这样加大了交易追踪难度，使得攻击者无法将交易记录与用户直接关联，从而加强匿名性。早起的混币服务借助可信第三方（trusted third party）来混合比特币地址，存在严重的局限性：需要保证足够多的资金在混合、运营者可以追踪资金、运营者窃取资金，或者倒闭后卷款而逃只能事后发现无法事前阻止。Mixcoin[9]试图通过信誉系统减缓这些风险。Blindcoin[10]用盲签名技术对混币进行进一步改进，保证运营者在提供混合服务时不能通过建立输入地址和输出地址的映射关系追踪资金流向，从而保护了用户相对于运营者的隐私，但仍不能阻止偷窃。CoinParty[11]提出的安全多方混合方案保证了只要有 2/3 的混合方是诚实的就安全。此外，为了避免可信第三方带来的中心化风险，第二代匿名技术应运而生[12]。

- 公平交换协议[13]：参与混淆的两方利用哈希锁定交易（hash-locked transaction）交换比特币。基本思想为 Alice 花费 Bob 的币，Bob 花费 Alice 的币，对 Alice 的花费行为感兴趣的攻击者观察到的不是 Alice 的交易，而是 Bob 的交易。
- CoinSwap[14]：交易双方（Alice 和 Bob）通过多个第三方托管交易，比如 Alice 要支付给 Bob 一定数量的币，则先将币转给 Carol，Carol 再将与这些币无关的等额币支付给 Bob。
- CoinJoin[15]：将 CoinSwap 中多个用户之间发送多个托管交易的设定改为他们共同生成一个合并后的交易，从而进一步混淆资金流。
- 隐蔽地址[16]：如果一个地址是公开的，那么任何人都可以查看这个地址进行过的所有交易。即便一个地址不是公开的，也可以知道这多笔交易是关联到同一个地址的。为了切断这种关联性，可以给每一个可能的发送者提供一个不同的比特币地址。但这么做有一定难度，所以隐身地址选择让接收者发布一个静态标识符（static identifier），这个标识符可以让每个发送者推出不同的与标识符比特币地址，且可以防止攻击者在现实世界的标识符和比特币地址之间建立联系。

这些技术不依赖第三方，不仅可以消除资金偷窃的风险，还可以省去混币费用。但在自行协商和执行混币过程中，参与用户可能面临协商过程中泄露信息、其他节点违规操作导致拒绝服务攻击等威胁。

2.1.3 基于匿名网络

1.3 中提到交易用户的 IP 地址也是可追踪的，所以光是隐藏交易数据是不够的，还需要将交易身份完全隐藏起来，匿名网络就能够使用户成为畅游网络的“黑影人”。匿名网络 Tor 给网络流量进行三重加密，将用户流量在世界各地的电脑终端间跳跃传递，难以追踪到流量的初始来源，达到网络匿

名访问的目的。Tor 在操作系统后台运行，创建一个代理连接将用户接入 Tor 网络，用户不仅可以匿名浏览网页和发送邮件，还可以用任何类型的在线服务掩盖自己的身份，匿名网络 Tor 和区块链技术结合起来，极大程度保护了用户的网络访问隐私。

2.1.4 基于盲签技术

已有工作[17]提出了解决比特币链上和链下交易匿名性问题的可行性方案，利用无需信任的第三方发行可赎回比特币的抵用券(voucher)，运用盲签(blind signature)技术和比特币合约(script)确保比特币与抵用券交换过程的匿名性和安全性，设计出实用的保护用户隐私的交易机制。这一匿名机制可在比特币软分叉后兼容，并保持可行性、安全性和匿名性特点。该方案提出了一个基于盲签合约模型的中介，用户通过将比特币转移给中介得到抵用券，将抵用券发给接收方，接收方再用抵用券与中介交易取得比特币。

交易过程采用盲签技术使得中介无法将抵用券与用户信息联系起来，即无法获知用户的交易信息，而链上合约保证了交易的公平性，即一旦用户发送了比特币给中介，中介就必须发行等价的抵用券，抵用券的唯一性保证币不会被双花。该机制将交易时间切成一个个固定片段，用户可选择进入服务的时间段，即中介同时服务多个用户，不同用户的交易混合在一起，互不影响。盲签技术确保抵用券具有不可关联性，合约性质保证比特币交易的公平交换。其中匿名交易机制分为两部分：链上匿名支付和混币、链下匿名支付。链上匿名支付使用了抵用券，链下匿名支付使用了微支付通道（micropayment channel network）。

该机制的创新性在于利用盲签技术和链上合约约束了中介的权利和行为。利用盲签技术，中介在签署抵用券时并不知道签名信息，也就是说中介无法将去盲化后的抵用券与签名用户联系起来，即使中介掌握了所有用户的签名记录，也无法将用户与交易关联。而且利用区块链合约规范交易条件，确保用户的交易安全性。合约可写定交易规则，如“当且仅当中介 I 在规定时间 t 内签署合法的抵用券，用户 A 才将比特币发送给中介，否则过了时间 t 后比特币返还给用户 A”，这样就能保证交易的公平性。

与传统的中介服务不同，该机制提供了多一层保障，即盲签技术防范了中介恶意泄漏数据的风险，区块链合约保证了交易资金的安全，从而用户无需信任中介。同时，用户有了更大的自由度，可自由决定抵用券的使用时间，也就是接收方可在任意时候赎回币。但这样的机制也有很多不足之处，比如中介被假定为“诚实但好奇”的，也就是中介不会拒绝用户请求，可是现实世界中中介有恶意拒绝服务的可能；不能保证链下交易的匿名安全；中介的集中服务更容易受到外界攻击盗取比特币。所以，该机制是在匿名程度上是比特币的进阶方案，但不能完全解决区块链隐私保护问题。

2.2 与比特币区块链兼容的匿名方案

除了在现成的比特币区块链上通过技术手段提高匿名性，研究者和开发者还提出各种新的区块链（数字加密货币），在隐藏交易内容的情况下实现区块链的特性（交易可验证、历史可追溯等）。

2.2.1 达世币

达世币（Dash）的私人交易（PrivateSend）功能就是基于 2.1.2 中的 CoinJoin 混币服务。用户将输入输出地址送到主节点进行混合，交易只能以规定面额（0.1, 1, 10, 100）为单位逆行，增加攻击者从金额大小猜测交易来源的难度。同时主节点保证乱序输出，外界很难从混淆后的交易中发现这笔交易。达世币还引入链式混合和盲化技术，解决主节点被外界攻击控制及信息泄漏的问题。前者是指用户随机选择多个主节点并在多主节点间混合后输出，后者是指用户随机选择一个主节点后，再转去另一主节点，后一主节点就难以获取用户的真实身份。除非攻击者同时掌控多个主节点，否则几乎不可能关

联指定交易。此外，达世币的被动匿名化方案，设定客户端以固定时间间隔发起交易参与主节点混合，避免攻击者根据用户交易习惯（交易时间）挖掘用户信息。

2.2.2 门罗币

门罗币（Monero）提出不依赖中心节点的加密混合方案，采用 2.1.2 中的隐蔽地址(stealth address)、环签名（ring signature）、环形保密交易（RingCT）技术保护用户隐私。隐蔽地址是将接受者地址用椭圆曲线加密算出一次性公钥保证地址每次都改变，解决地址关联性问题。环签名是在交易上加入其他用户的公钥签名，外界就不知道发起者是谁，而且私钥映像是一次一密，保证不可追踪性。环状保密交易技术则可以隐藏交易地址和交易金额。

2.2.3 零币

恶意用户参与环签名会暴露隐私，为避免这一风险，零币协议[18]（Zerocoin）的思路就是利用零知识证明，让用户只通过和加密货币本身进行交互来隐藏交易信息。零币是第一个提出通过去中心化电子现金方案（decentralized e-cash scheme）解决比特币匿名性问题的，它既不依赖于电子签名来验证，也不需要中心化的银行或发行方来防止双花问题。

零币的基本构造是用户 Alice 在挖币之前先生成一个随机的“序列号（serial number)”S，然后用安全电子承诺方案（secure digital commitment scheme）生成 S 的“承诺（commitment）”C，只有通过参与生成 S 的随机数 r 才能使之公开。承诺其实也是一个币，Alice 将其“贴在公告栏”上，如果它的构造和金额是正确的，就会得到所有用户的采纳。Alice 下次想要消费时，需要从公告栏里“兑现”她的承诺，就可以从公告栏上获取所有有效承诺的列表，并提交一份非交互式的零知识证明（non-interactive zero-knowledge proof）给所有用户验证，以表明她知道 C 在这份列表中，而且她知道一个数值 r 可以通过 C 得到 S。最后她广播 S，如果没有在之前的交易中出现，就可以证明她没有双重消费。这份协议达到了两个重要的目标：他人无法将 Alice 挖出的币和她取回的资金联系起来，从而保证了隐私性；Alice 如果双重消费就会被他人发现，从而保证了可靠性。

比特币解决双花问题是通过验证者扫描 UTXO，如果一笔交易的输出已经列入为其他交易的输入，则无法再次被支付。零币解决双花问题则是通过验证者扫描序列号列表，如果序列号已经在之前的交易中出现，则这笔交易无效。

零币协议是与比特币协议相容的，事实上区块链可以发挥“只增不销”的“公告栏”的作用，既可以储存信息，也可以处理交易。Alice 托管资金（添加承诺）可以在区块链上进行，遵照严格的协议条件来确定何时可以访问她承诺的资金。尽管零币可以直接部署在比特币区块链网络上，但由于没有获得比特币社区的同意，开发团队创建了一个独立于比特币的匿名数字货币 Zcoin。

零币的匿名性仍然有局限性。首先，由于攻击者可以观察到被挖出的币和被花费的币的数量，最坏情况下当 N 枚币被挖出，且这 N 枚币已被陆续被花费时，如果又有一枚币挖出，则等待被花费的匿名币集合的大小仅有 k=1，那么很显然这枚币的匿名性就大打折扣了。零币提供的匿名性下界是一枚币在挖出和花费之间有被诚实方挖出的币的数量，上界是被挖出的币的全集大小。其次，挖出和花费的币的数量对系统里所有用户都是公开的，为攻击者提供了潜在信息来源。不过之前的电子现金方案是向商家和银行披露这些信息的，相比之下零币是有进步的，因为在大多数电子现金模型中银行通常被认为是对立方，而且零币还消除了信息不对称。最后，零币没有隐藏交易金额信息。

2.2.4 零钞

文章[19]介绍了零钞协议（Zerocash），阐述和构造了去中心化匿名支付（Decentralized Anonymous Payment, DAP）方案。DAP 方案能够让用户私密地直接向他人进行支付，而且相应的交易隐藏了支付的发送方、接收方和转账金额。因此零钞在零币的基础上更彻底地实现匿名性。

DAP 方案的构造借助了简洁非交互零知识证明系统（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, zk-SNARK）。zk-SNARK 可以被视为一个黑箱子，由一个可信方一次性生成两个公钥：证明钥匙和验证钥匙，即便是不可信的证明者也可以拿着证明钥匙生成一份对一个 NP 陈述，即他拥有某些知识的证明，这份证明是零知识的，且无需交互。任何人都可以拿着验证钥匙，不通过与证明者的任何接触即可证实这份证明。zk-SNARK 的内部构造涉及了同态加密、多项式恒等测试、椭圆曲线加密等理论。

零钞协议（DAP 方案）提出了浇铸（pour）操作和铸币（mint）操作。浇铸操作用来花销钱币，将一个旧币铸成多个新币，且输入输出总和相等，每个新币有独有的密钥、金额、序列号。铸币操作是往托管池（即 2.2.3 中的公告栏）中注入钱币并写下承诺（commitment），用户在花费时需要给出钱币的序列号，并证明自己知道该承诺的用户私钥。这样用户就在完全不暴露身份下进行交易，而序列号的唯一性保证货币不能双花。

尽管开发团队根据零钞协议创建的 Zcash 是数字加密货币（cryptographic currency）中匿名性最好的，其安全性依赖于初始化参数的随机性和绝对销毁。如果希望减轻这个步骤的信任要求，可以通过安全多方技术进行初始化。

3 区块链应用的隐私保护

区块链的价值不仅仅体现在数字加密货币中，还体现在各种落地应用中，比如去中心化文件存储、去中心化物联网和智能合约。研究者和开发者也开始关注区块链应用如何在提供用户服务的同时，保护用户的隐私。

3.1 去中心化文件存储

在隐私保护意识日益加强的今天，用户对于没有提供充分隐私的云存储服务商存在着担忧。在区块链被提出之前，就有点对点（peer-to-peer, P2P）隐私保护存储系统 Freenet[20]。但 Freenet 存在一个问题，就是用户为系统中其他参与者贡献存储容量的动力不足。针对这一点，文章[21] 提出，在分布式存储的基础上，结合基于区块链的支付系统，在激励用户参与的同时保护用户隐私。其中隐私保护基于的是可链接环签名（linkable ring signature）。

3.2 去中心化物联网

物联网是指通过互联网连接多个实物的网络，由于这些互联的设备（实物）在交流的过程中会传播敏感的私人信息，暴露使用者的行为和偏好，因而存在隐私问题。文章[22]提出了结合区块链和 P2P 存储系统的设计好的私人物联网（private-by-design IoT）。在 IoT 设备之间产生和交换的敏感数据存储在 P2P 存储系统里，可以保证隐私性和鲁棒性。区块链则用于注册和认证各种操作（创建、修改、删除），确保数据的真实性和防止未经授权的访问。

3.3 智能合约

Zerocash 利用零知识证明工具 zk-SNARK 实现了完全匿名的转账功能。但它像比特币一样，无法实现复杂的转账逻辑。以太坊在比特币的基础上，通过定义了一个图灵完备的脚本语言，允许用户在链上实现更为复杂的转账逻辑，允许用户发行自己的代币，部署分布式应用（智能合约）等。

如何将数字货币转账的匿名性扩展到智能合约的匿名性，是一个很有价值的问题。当前智能合约中的参数是对全网公开的，任何人可以从一些链上查询工具很容易地查看任何和智能合约交互的账户，利用一些反向工程，还可以查看执行的具体细节，毫无隐私可言。

在文章[23]中，介绍了一种无状态隐私保护的智能合约机制 HAWK。它允许合约开发者利用文章所提供的开发工具编写合约规则并部署到区块链上。HAWK 的合约是由一个指定节点执行而非去中心化执行的，在部署的时候，需要指定合约执行者的公钥。参与者将自己的输入用公钥加密后写在链上，合约执行者执行完毕后执行者再将结果使用用户的密钥加密写到链上。整个过程利用零知识证明过程在保护隐私的前提下保证正确性。

参考文献

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” http://bitcoin. org/bitcoin. pdf, 2008.

[2] T. B. Lee, “A risky currency? Alleged $500,000 Bitcoin heist raises questions,” Available at http://arstechnica.com/, June 2011.

[3] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system." *Security and privacy in social networks.* Springer, New York, NY, pp.197-223, 2013.

[4] P. Koshy, D. Koshy, and P. McDaniel, "An analysis of anonymity in bitcoin using p2p network traffic." *International Conference on Financial Cryptography and Data Security.* Springer, Berlin, Heidelberg, 2014.

[5] E. Androulaki, G. O. Karame, G. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin." *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2013.

[6] S. Ranshous, C. A. Joslyn, S. Kreyling, K. Nowak, N. F. Samatova, C. L. West, and S. Winters, "Exchange pattern mining in the bitcoin transaction directed hypergraph." *International Conference on Financial Cryptography and Data Security.* Springer, Cham, 2017.

[7] G. Di Battista, V. Di Donato, M. Patrignani, M. Pizzonia, V. Roselli, and R. Tamassia, "Bitconeview: visualization of flows in the bitcoin transaction graph." *2015 IEEE Symposium on Visualization for Cyber Security (VizSec)*. IEEE, 2015.

[8] J. D. Nick. Data-driven de-anonymization in Bitcoin. MS thesis. ETH-Zürich, 2015.

[9] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for Bitcoin with accountable mixes." In *International Conference on Financial Cryptography and Data Security*, pp. 486-504. Springer, Berlin, Heidelberg, 2014.

[10] L. Valenta, and B. Rowan. "Blindcoin: Blinded, accountable mixes for bitcoin." In *International Conference on Financial Cryptography and Data Security*, pp. 112-126. Springer, Berlin, Heidelberg, 2015.

[11] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, "Coinparty: Secure multi-party mixing of bitcoins." In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, pp. 75-86. ACM, 2015.

[12] M. Möser, and R. Böhme. "Anonymous alone? measuring Bitcoin’s second-generation anonymization techniques." In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 32-41. IEEE, 2017.

[13] S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to better—how to make bitcoin a better currency." In *International Conference on Financial Cryptography and Data Security*, pp. 399-414. Springer, Berlin, Heidelberg, 2012.

[14] G. Maxwell, "CoinSwap: transaction graph disjoint trustless trading," https://bitcointalk. org/index. php, 2013.

[15] G. Maxwell, "CoinJoin: Bitcoin privacy for the real world," https://bitcointalk. org/index. php, 2013.

[16] P. Todd, "Stealth addresses. " Post on Bitcoin development mailing list, https://www. mail-archive. com/bitcoindevelopment@ lists. sourceforge. net/msg03613. html. 2014.

[17] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions." In *International conference on financial cryptography and data security*, pp. 43-60. Springer, Berlin, Heidelberg, 2016.

[18] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin." *2013 IEEE Symposium on Security and Privacy*. IEEE, 2013.

[19] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin." *2014 IEEE Symposium on Security and Privacy*. IEEE, 2014.

[20] I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong, "Freenet: A distributed anonymous information storage and retrieval system." *Designing privacy enhancing technologies*. Springer, Berlin, Heidelberg, 2001.

[21] H. Kopp, D. Mödinger, F. Hauck, F. Kargl, and C. Bösch, "Design of a privacy-preserving decentralized file storage with financial incentives." *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2017.

[22] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review." *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. IEEE, 2016.

[23] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts." *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016.