SUPER ZERO(SERO)
技术白皮书

全球首发隐私保护一站式平台

让分布式应用真正的安全、隐私、稳定

SERO

Version 1.10

Last Update: Jan 10th, 2019

第一章 前言和概述

互联网飞速发展让信息的流转速度变得非常高效，从而推动了人类社会的发展，但从另外一方面看，隐私问题也正是因为互联网的高速发展而变得更加严重。区块链作为下一代的价值互联网，曾被认为是保护隐私非常好的工具，但大家很快发现，当前主要的区块链网络中，一旦数字钱包地址和它的拥有者的个人信息对应起来，该钱包的拥有者所有账户信息、交易信息都将在整个网络中一览无遗并且无法消除，这会导致比互联网的隐私泄露更加严重的问题。为此区块链行业的密码学和顶尖的技术专家都在进行不懈努力，业界有几支团队研发了一些保护隐私的特殊虚拟货币，这类虚拟货币被称之为“匿名币”，行业中比较有名的数字货币包括大零币 Zcash (ZEC)，门罗币 Monero (XMR)，达世币 (DASH)等，这些采取了一定隐私保护的数字货币基于其巨大的市场需求，均获得了非常高的流通市值，排名在全球20大虚拟货币之列，说明隐私保护对区块链行业而言是一个非常强烈的需求。

智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。区块链上图灵完备的智能合约系统，可以满足开发者编写任意复杂的，存在于区块链上并且能被区块链传递的合约。开发者可以用智能合约开发语言实现比如定制货币、金融衍生品、身份系统和去中心化组织等功能，极大的扩展了区块链系统的适用范围。智能合约是价值互联网重要的的技术基础之一，但是目前令人沮丧的情况是，全球目前运行的区块链系统均不支持对智能合约加密保护，现有的隐私保护机制使用场景受到这一技术限制的影响被极大的缩小了其适用范围。区块链技术起源于中本聪发明的比特币，被视为区块链1.0，让人类世界找到了数字虚拟货币这一巨大的财富；而当以太坊面世后，智能合约的发明让区块链技术的落地变得更为可行，从此基于区块链技术的去中心化分布式应用（简称“DApp”）成为可行，这让区块链技术可以被运用到更多的行业中，因此以太坊被视为区块链2.0。同样可以类比，如果Zcash和门罗币为代表的不支持智能合约的匿名区块链系统是隐私保护方案1.0的话，为了让方案可以落地到更多行业和应用场景中去，支持智能合约的隐私保护方案2.0备受期待。

不可否认的是，支持智能合约的匿名区块链系统具有非常高的技术门槛，全球仅有屈指可数的团队正在为之努力，如今Super Zero（简称“SERO”，中文：超零币）也正式向全球进行产品发布，SERO的研发团队（简称“SERO团队”）也是目前全球唯一能就该问题提出完整的解决方案，并已经完成主要工程研发工作的团队。不仅如此，SERO团队并没有将成功研发支持智能合约的隐私保护区块链系统作为去中心化应用的隐私保护方案的终点，为了让受到隐私保护的去中心化应用的广泛落地成为可行，SERO团队不但考虑到了保护DApp使用者的账户隐私、相关令牌（Token）和私有数据传递过程的隐私，同时充分考虑到了在区块链系统数据传

输过程中，之前受各层传输层协议限制的隐私保护策略，甚至还包括了去中心化应用和互联网应用相结合场景下的数据隐私保障。

为此，SERO团队设定了一个能为去中心化应用提供完整隐私保护解决方案的三件套项目，包括SERO（支持智能合约的匿名区块链系统）、异形协议（一个能解决去中心化网络信息传输的协议）以及卡斯特罗协议（保护去中心化网络，以及为互联网交互的各节点提供隐私保护的协议）等尖端创新科技组件。**最近SERO已经完成了核心的研发工作，包括隐私保护相关协议，和图灵完备的链上运行智能合约**，本白皮书主要就SERO的工作进行说明，并包含了该项目的一些基本情况以及披露后续的项目计划。

第二章 SERO介绍

2.1 去中心化技术与隐私问题

当前，用户对隐私保护的关注和需求日益加剧，多家知名公司都先后被爆出泄露了大量用户隐私数据，包括雅虎、优步、Paypal、洲际酒店集团、美信用机构Equifax、英国国家医疗服务体系（NHS）等等，相关泄露数据涉及几千万到数亿规模的用户。Facebook也因为2018年3月份发生的一次最大规模的隐私泄露事件，市值在两天内蒸发掉数百亿美元，并有可能面临高达其四倍市值的天价罚款。隐私问题同时也引起了很多国家政府的重视，欧盟率先颁布《通用数据保护条例》(GDPR)就是一个旨在为了督促各家公司有效保护用户隐私的法案。

不得不说互联网带来了许多隐私泄漏问题，而互联网应用场景中大部分的隐私泄漏往往是由于中心化的平台缺乏足够的数据安全保护机制引起的。隐私区块链系统被认为能从根源上杜绝此类事件的发生，然而比特币和以太坊等区块链网络的设计其实并没有考虑当去中心化网络与使用者现实身份结合后，区块链上存储的用户数据会产生用户的隐私泄漏问题。区块链网络中数字资产及其交易记录等异常敏感的信息，对所有人透明并且是不可篡改的，当区块链在现实场景中进行大量的应用的真正落地时，对大部分场景需求来说，这点无疑是不可接受的。

财务隐私合法使用案例的范围很广。事实上，财务隐私对于世界上发生的大多数交易来说应该是需要的，数字货币相关账户的资产和交易的隐私数据通过区块链上存储的交易记录暴露在所有人面前是不合理的。

现实世界中遇到的相关合理需求举例如下：

* 一家公司想要保护不让竞争对手知道的供应链信息；

* 个人不想被公众知道她正在支付向破产律师或离婚律师咨询的费用；

* 一个富有的人，不希望让潜在的犯罪分子了解他们的行踪以及试图勒索他们的财富；

* 不同商品的买卖双方希望避免交易被他们之间的中间商公司切断；

* 投资银行、对冲基金和其他类型的交易金融工具（证券、债券、衍生工具）的金融实体，如果其他人可以弄清楚他们的仓位或交易意图，那么这些信息的暴露会使交易执行者处于劣势，影响他们盈利的能力。

在智能合约中，整个行为序列通过网络传播并记录在区块链上，所以是公开可见的，许多个人和组织认为金融交易（例如保险合同或股票交易）是高度机密的，比如多方之间基于某些条款的细节产生的交易，原本可能需要当事人的信息保护，现在却无法做到。所以，缺乏隐私是广泛采用去中心化智能合约的主要障碍，隐私保护技术的匮乏已经成为了去中心化应用普及落地的严重瓶颈，故而相关领域的技术发展进程也备受公众关注。

2.2 区块链隐私泄漏风险

比特币网络是典型的区块链技术代表，目前市场上主流的加密货币，几乎都基于与之相同的技术特点，下面以比特币网络为例分析隐私泄漏的风险。

首先从比特币交易系统的结构设计来看：

* 交易数据的UXTO模型包含输入地址和输出地址信息，每一个输入地址都指向前一笔交易，所有输入资金都能够追溯到源头。
* 交易数据存储在公开的全局账本中，任意参与用户都可以获得完整的全局账本。其在共识过程验证节点需要检索历史交易，所有的交易信息没有采用加密等手段保护数据。

比特币交易参与方的地址都是由用户自行创建且与身份信息无关的，任何人都无法直接通过观察交易记录推测出交易中用户的身份信息。但全局账本公开的交易之间存在关联关系，潜在攻击者可以通过分析全局账本中的交易记录推测出比特币地址的交易规律，包括相关地址的交易频率、交易特征、地址之间的关联关系等。基于这些规律，攻击者有可能将比特币地址和特定用户在真实世界中的身份相关联。

其中一种方式主要通过分析地址相关的交易记录，获得该地址交易的规律特征，据此推测对应用户的身份信息。由于在某一特定类型的区块链交易中会存在它特有的交易特征，攻击者可以根据地址的交易特征，对其交易发生的真实场景进行还原，从而做出用户真实身份的推测。 Androulaki E.等人设计了一个匹配区块链地址与学生身份的模拟实验，学生以比特币作为日常交易的支付手段，并使用比特币推荐的一次性地址方法加强隐私保护，分析人员通过基于行为的聚类技术，能够以42%的准确率将学生身份和区块链地址成功匹配。Monaco J. V.等人将比特币用户的交易行为进行量化，以交易时间间隔、资金流向等12个维度为依据分析用户的交易规律，经过6个月实验得到的大量数据表明，利用这种分析模型成功识别用户真实身份的精度高达62%，错误率低于10.1%。

另一种方式则主要利用区块链交易设计中存在的一些潜在知识，实现对不同地址的聚类，得到同一个用户的多个地址。

针对地址聚类目前主要有以下3条聚类规则。

*对于一个具有多输入地址的交易，通常认为所有的输入地址都来自同一个用户个体或用户的集合。当用户发起一次交易时，资金可能来自于用户的多个地址，而多输入交易中用户需要对每个输入地址单独进行签名，因此大多数多输入交易的输入地址来自同一个用户。这项规则已经应用于很多研究中，取得了很好的聚类效果。

* 在矿池组织的交易中，同一个交易中的多个输出地址属于同一类用户集合。随着“挖矿”难度的增加，个体“矿工”已经无法在竞争中获胜，需要成百上千的“矿工”加入“矿池”共同完成一次“挖矿”，得到的奖励会分配给参与集体“挖矿”的“矿工”。

* 交易中找零地址和输入地址隶属于同一个用户。在一次交易中，输入地址中的总金额可能会大于用户发出的金额，因此比特币系统会为发送方自动产生一个找零地址，用于接收交易中的找零资金。找零 地址与其他地址一样都有可能被系统选择成为新的交易中的输入地址，但作为输出地址的情况一般只会出现一次。由于找零地址在交易发生时是由系统重新生成的，因此一个地址不可能同时作为一次交易的 输入地址和输出地址，交易的输出中也必然存在找零地址以外的输出地址。利用找零地址的这些特征，可以发现更多地址之间的关联关系。

目前已经有很多研究利用上述聚类规则，发现了比特币系统中很多地址之间的关联性。Meikle John S.等人通过使用启发式聚类方法实现了对比特币盗窃案件中相关比特币地址的识别。Dmitry E.等人也提供了一个方法，可以对比特币地址进行自动聚类。

2.3 去中心化隐私保护技术

我们很高兴地看到现在有一些团队开始关注到去中心化网络的隐私保护问题，比较著名的项目包括 Zcash，门罗币和达世币。

一种广泛应用的方法是在不改变交易结果的前提下改变交易过程，使攻击者无法直接获得交易的完整信息，这种方法被称为“混币”。譬如在Chaum D.的文章里提到了一种匿名通信技术，在通信过程中隐藏了真实的通信内容，基本思想可以通过式(1)表达:

$$\mathbf{C}M\left(Z1, \mathbf{C}A\,(Z0, m), A\right) \; -> \; \mathbf{C}A\,(Z0, m), A \qquad (1)$$

式 (1) 左侧为发送方发给中间人的信息，右侧为中间人将信息处理后发送给接收方的消息。发送方想要将消息 $Z0$ 和 m 发送给接收方的地址A，首先使用接收方的密钥 $\mathbf{C}A$ 对消息进行加密得到$\mathbf{C}A\,(Z0, m)$，然后将中间人的验证消息 $Z1$、加密后的消息$\mathbf{C}A\,(Z0, m)$和接收方地址 A 进

行打包，并使用中间人的公钥 CM 进行加密，防止信息在发送过程中被攻击者截获或篡改。中间人收到信息后使用自己的私钥进行解密，得到 $Z1$, CA ($Z0$, m), A，但无法解密CA ($Z0$, m) 的内容。中间人在验证 $Z1$ 无误后，将 CA ($Z0$, m) 发送给地址 A 。接收方使用自己的私钥解密消息，完成此次通信。

利用这种方法，消息没有在发送者和接收者之间直接传递，而是通过中间人间接传递，使攻击者无法观察到真实发送者和接收者之间的通信行为，提高了通信的匿名性。若将消息通过多个中间人进行传递，攻击者发现双方通信关系的难度将大大增加。

数字货币中的混币机制借鉴了上述思想（如DASH和门罗币），通过中间层级结构，切断交易中真实的发送方和接收方的被可追踪的关联。混币过程的执行可以由可信的第三方或某种协议实现。根据混币过程中有无第三方节点参与，可将现有的混币机制分为两类：基于中心节点的混币机制和去中心化的混币机制。这两种机制在混币可靠性、混币效率和混币成本等方面各有优势和缺陷。

不过随着技术的发展，更为尖端的加密学的技术被应用到区块链隐私保护中，譬如 Zcash 对零知识证明的应用。

以下就目前3种最为流行的隐私保护的加密货币稍作说明：

Zcash

Zcash 是一种加密货币，使用加密技术为其用户提供比其他数字货币（如比特币）更强的隐私。 最初是由一个命名为 Zerocoin 的协议发展而来，随后其团队开发了 Zerocash 系统，直到2016年将其发展为 Zcash 加密货币。

Zcash 的交易在公共的区块链上发布，但用户可以使用可选的功能隐藏区块链上交易的发送者、接受者及交易金额。只有那些拥有查看密钥(VSK)的人才能看到交易的内容。用户拥有完全的控制权，他们可自行选择是否向其他人提供查看密钥，以用于审计目的。

Zcash是基于比特币的基础架构开发改进的，并采用了一种叫zk-SNARKs的零知识证明技术实现了对用户信息的加密。zk-SNARKs是基于纯数学理论实现的加密手段，和区块链的本质一样，这种方式的好处在于使用它不需要依赖外部的运行环境而自成体系，因而具备十分广泛的应用场景。

然而，由于Zcash采用了和比特币网络相同的底层架构，因此虽然能够实现隐藏交易时发送者，接受者和交易金额，但它只能支持简单的交易，简单讲就是一个预置了隐私保护机制的比特币网络。除此之外，整个运用零知识证明对交易进行加密的过程的性能比较低效，也使其应用场景进一步被限制。

Monero

Monero 创建于2014年4月，与 Zcash 不同的是它并没有选择基于之前的区块链系统开发，并从底层实现有着很好的模块化设计，因此具有比较好的扩展性。

Monero 的特点在于首先它虽然也采用了工作量证明（POW）的共识机制，但是与之前的许多加密货币不同，Monero工作量证明算法CryptoNight是为AES密集型和很耗内存的操作，这显著降低了GPU对CPU的优势，换句话说降低了工作量证明算力集中化的风险。

另外在加密手段方面，它采用的是环形签名（Ring Confidential Transactions）算法，首先将签名者的公钥与另外一个公钥集合进行一起混合，然后对消息进行签名，使得外界无法区分集合中哪个公钥对应真正的签名者，从而达到保护用户真实身份的效果。Monero的混币参与用户无需与其他参与节点进行交流，可自行参与混币，为去中心化混币机制中常见的拒绝服务攻击、混币用户泄露信息等问题提供了有效的保护措施。

但Monero同样不支持智能合约，另外虽然其采用去中心化的混币技术，仍然存在较高的被攻击风险，用户在使用环签名技术时，需要依赖其他用户的公钥，如果其他用户是恶意的，则会在一定程度上导致用了用户的隐私泄露问题。

Dash

Dash是第一个以保护隐私为目的设计的数字货币，它采用的中心化混币方案的本质是单纯地将一笔资金在多个地址中进行多次转移，实现简单，易于操作，混币过程不需要其他的技术支持。中心化混币方案在各类数字货币系统中具有极高的适用性，但是，现有的方案要求参与混币的人员在线进行混币。如果双方就混币的数额不能达成一致的话则必须推迟，为了使得混合充分，交易普遍存在时延问题并且混币器是中心化部署的，混币器节点能获取交易的所有信息，能盗币。中心化混币方案的大多数改进方案是通过增加第三方违规的代价来防止盗窃和信息泄露的发生，不能从根本上杜绝违规行为的发生；采用盲签名等密码学技术的混币方案会增加计算代价，并且由第三方执行混币过程必然会带来额外的服务开销。

遗憾的是，Dash同样不支持智能合约，并且第三方的混币提供者这样的机制依赖于第三方的可信度，同样面临不可预测的风险。近年来，Dash基于其前期良好的流通性，着力于生态应用的开发布局，并加强了和企业间的合作，力图将Dash币打造成具备较强流通价值的支付工具，而不再强调其隐私保护方面的优势。

总结

从最新的技术发展来看，通过采用最新的密码学算法保证隐私功能，例如非交互式零知识证明机制（NIZK）是最有前景的一种改进。但引入加密机制需要对底层协议进行大幅改动，并需要消耗更多的计算资源，影响区块链应用的效率，因此引入的隐私保护机制需要充分考虑节点在计算和存储上的性能、效率和成本。

在去中心应用方面，以太坊的智能合约大大增加了区块链系统的应用场景，而不再仅仅局限于其流通的数字货币价值。然而目前主流的区块链隐私保护技术均不支持智能合约，从而无法建立实用并且落地的去中心化应用。因为任何一个安全的隐私保护机制要支持智能合约，都涉及到对区块链底层系统做出重大的修改工作，因此一直难以落实到实际系统实现中。

面对以上问题，SERO是一个很好的解决方案。

2.4 SERO解决方案概述

SERO（Super Zero，超零系统）是全球首个通过非交互式零知识证明(NIZK)，真正实现具有图灵完备智能合约的隐私保护的区块链系统，和现有的区块链隐私保护技术相比，SERO不仅能实现对账户信息和交易信息的隐私保护，还能实现对图灵完备的智能合约输入输出的隐私保护，另外，开发者还能基于SERO-Chain上的智能合约发行的匿名数字资产（Token），并且与智能合约的通讯信息也同样会得到隐私安全保护。

SERO重新设计了区块链结构和各类底层协议，使得对隐私保护的图灵完备智能合约成为现实，不仅使更广泛的应用场景获得了隐私保护措施，并且因为其采用的先进的NIZK加密学算法，也进一步提升了对用户隐私数据的攻击难度。除此之外，在即将发布的V1.0版本中，改进了目前NIZK加密算法的实用性问题，大大降低了所需要消耗的内存资源，提升了计算效率。除此之外，对比市面上的主流匿名区块链系统，SERO对图灵完备的智能合约的支持和对其相关的去中心化应用的隐私保护措施，使其使用场景得到了极大的泛化。

更值得一提的是，SERO团队不仅考虑到了去中心化应用本身所需要的隐私保护措施，而且还从应用落地的角度，计划从点对点的网络传输安全以及账户物理的网络地址的隐私性角度提供解决方案，可以使与中心化应用交互时，或者与使用者客户端交互式时也能获得强大的隐私保护功能。

整个综合解决方案会由三位一体的全套套件构成，其中SERO是第一个公开发布的项目，另两个项目的定位分别如下：

异形协议 （Alien Protocol）：一种分布式的DNS系统，可以利用现有的P2P网络交互信息，具备IP自动切换和动态寻址的功能，抗攻击者阻断，使整个数据传输网络具备十分稳定的安全性。

卡斯特罗协议（Castrol Protocol）：通过去中心化网络的方式，实现对IP地址的匿名保护，可同时运用于中心化和去中心化网络的物理节点的隐私保护。

第三章 SERO的设计

3.1 设计原则

正如前文所说，现有市场存在的去中心化网络的隐私保护技术，并没有跟去中心化应用相结合，尤其是没有对智能合约的执行进行隐私保护。在智能合约中执行的动作序列，通过网络传播和/或记录在区块链上，是公开可见的。在图灵完备的区块链网络中，SERO的设计，在满足系统能力需求的同时，还必须满足几个基本的原则。

不可追踪性，区块链网络中的每一笔交易都具有输入和输出，如此一来，就构建了一个交易的有向无环图，在这个图上可以跟踪所有的交易流向，所有的交易序列都能被串联起来，并以此溯源。SERO的设计中要将两个交易之间的链接断开，使攻击无法进行。

不可关联性，区块链网络中每个用户都有自己的收款地址，一旦这个地址跟真实的用户身份关联，那么，在网络中这个地址发生的所有交易，都能关联到这个身份上，该地址一切的行为都暴露无疑。即使用户可以创建新的假名公钥以增加其匿名性，每个假名公钥的所有交易和余额的值都是公开可见的。SERO通过加密技术手段使收款地址无法被关联。

抗统计分析，真实用户的行为具有统计特点，如果区块链网络中的交易数据之间具有反应这样统计特点的关联性，通过对区块链数据的统计分析，就能够一定几率推测出这些地址发生的交易是属于某个特定用户的行为。即使是采用环签名，在面临有作恶的环成员或者节点的时候，抵抗统计分析的能力将会下降。SERO需要通过技术手段将地址以及地址之间的关系完全隐藏。

实用性原则，SERO在对交易数据进行隐藏的同时，并不会一股脑的将所有的信息都纳入范围内，这样做是不经济并且运行效率低下的。SERO会兼顾用户已有的使用习惯和痛点，进行阶段性研发。

可选的审计方案，对于某些较为复杂的商业应用领域，用户可能需要有一个完全信用的第三方对他发生的所有交易进行财务方面的审计，这时，他应该可以做出选择，决定是否给予第三方一个跟踪他所有交易具体信息的能力。

3.2 实现方案

在第一期的计划中，SERO通过非交互零知识证明(NIZK)，将交易体系的输入和输出以及交易细节完全隐藏起来，除了交易双方，其他任何人对这些隐藏细节完全是不可见的。同时，因为考虑到线上运行智能合约以及公开合约发行资产总数具有普适性的适用性，SERO会保留链上运行的智能合约，将智能合约所产生的资产与SERO本身的交易体系融合，以此来实现智能合约所产生资产的隐私性。

在第二期的计划中，对于具有隐藏合约发行资产总数的需求，我们将在线上运行智能合约内部提供一种名为隐匿数据的隐藏结构，同时只在链下对这种隐匿数据进行计算。以此来实现隐藏合约发行资产总数的功能。

在第三期的计划中，我们会采用更为先进的共识机制，提升SERO网络的吞吐量。同时，对于具有隐藏合约内部计算规则的需求，我们会将合约的运行分解为线下计算和线上验证两个步骤，线下计算完全了解运算规则和数据，并给出运算后的加密结果，当这个结果提交到线上时，线上节点只会对结果进行有效性验证，以确定其中包含的数据是否符合运算规则，但节点并不知道这些数据和运算规则的详细信息。

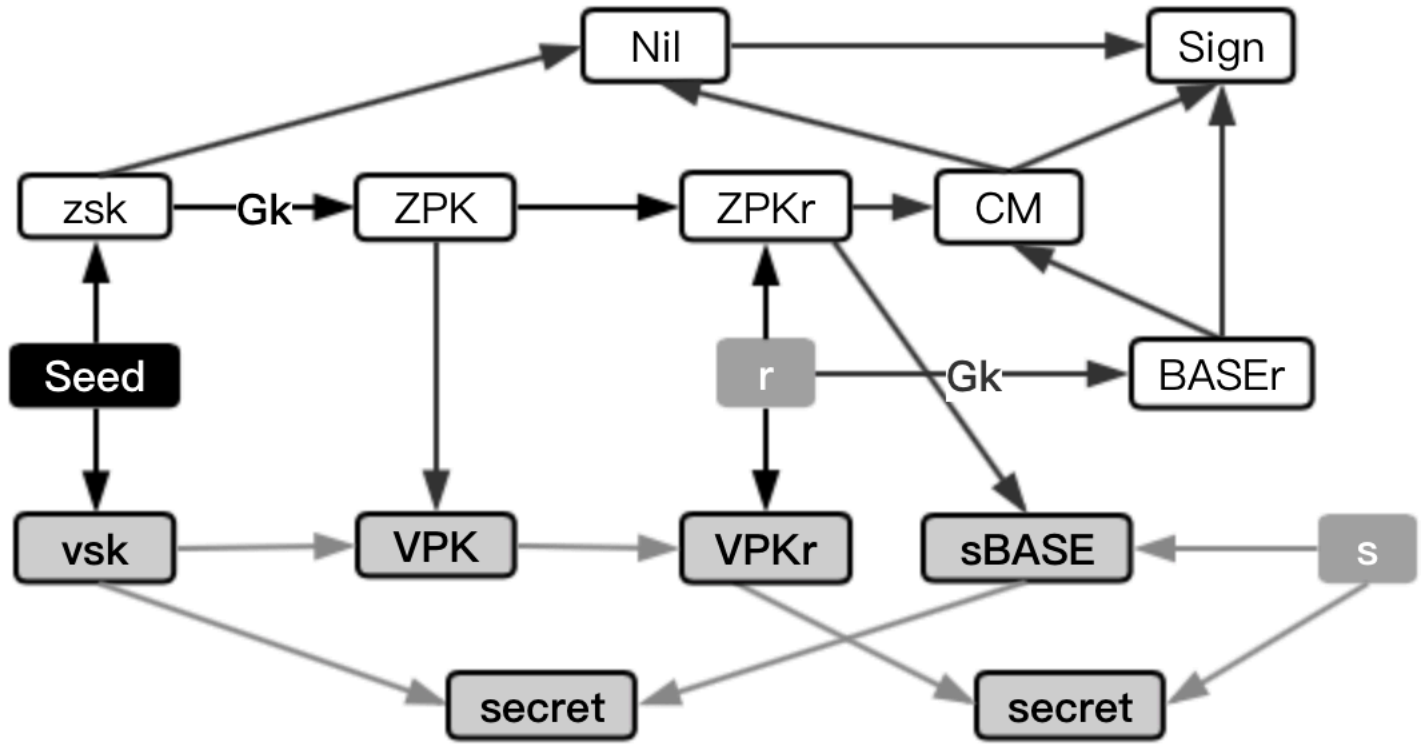
3.3 SERO协议

账户系统(Account System)

账户系统分为两个种类：用户账户和合约账户。用户账户是用户选定一个32byte的$Seed$，而合约账户根据用户安装智能合约的环境产生一个64byte的地址，两者都是系统唯一，不可重复的。

用户账户可以产生一个64byte的私钥SK和一个64byte的公钥PK，该公钥是用户的付款地址。在安装或调用智能合约时，钱包会根据当前情况生成一个暂存地址PK_r，这个暂存地址无法用任何方式关联到用户的私钥和公钥，并且只会使用一次。

在智能合约安装的时候，钱包会根据当前情况，将暂存地址转为64byte的智能合约地址（$CADDR$）。当节点收到地址时，需要确保智能合约地址之前没有出现过。



$Let:$

$G_k = NewEcc()$

$seed = New(Byte32)$

$r = RandFr()$

$s = RandFr()$

$a = RandFr()$

$m = Message()$

$SK:$

$zsk = HASH_{zsk}(seed)$

$vsk = HASH_{vsk}(seed)$

$sk = (vsk, zsk)$

$zvsk = zsk \cdot vsk$

$PK/TK:$

$ZPK = zsk \cdot G_k$

$VPK = vsk \cdot zsk \cdot G_k$

$PK = (ZPK, VPK)$

$TK = (ZPK, vsk)$

$PK_r:$

$$BASE_r = r \cdot G_k$$

$$ZPK_r = r \cdot ZPK$$

$$VPK_r = r \cdot VPK$$

$$PK_r = (VPK_r, ZPK_r, BASE_r)$$

$Trace$:

$$VPK_r == vsk \cdot ZPK_r$$

Enc :

$$BASE_s = s \cdot ZPK_r$$

$$SECRET = s * VPK_r$$

$$key = Hash_s(SECRET)$$

$$M = Enc_{vk}(m, key)$$

Dec :

$$SECRET = vsk \cdot BASE_s$$

$$m = Dec_{vk}(M, key)$$

$Sign$:

$$k = Hash_1(a, zvsk, m)$$

$$s0 = k \cdot BASE_r$$

$$h = Hash_2(S0, m)$$

$$s1 = k + zvsk \cdot h$$

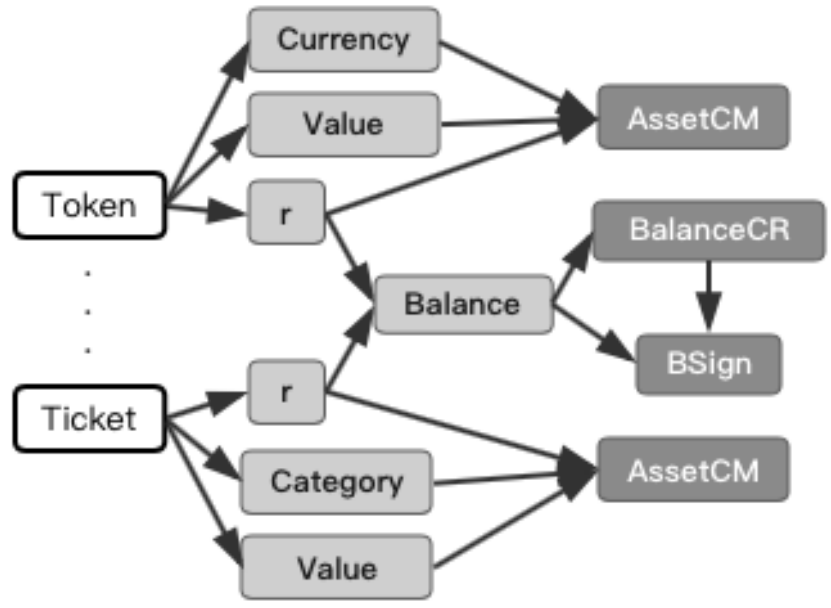
$$sign = (s0, s1)$$

$Verify$:

$$s1 \cdot BASE_r == S0 + h \cdot VPK_r$$

$Seed$是账户种子，用户必须妥善保存。SK是私钥，不可持久化存储，其中TK是跟踪私钥，可以提供给可信的第三方用作账户的审计。PK是公钥，提供给其他用户的交易目标地址。PK_r是暂存地址，提供给智能合约，用来临时接收资产的目标地址。

资产系统(Assets System)



Let :

$G_r = NewEcc()$

$H_{for\_o} = Hash_{for\_o}()$

$Token$:

$token = (value, Currency)$

$G_{cy} = Ecc(Currency)$

$r_{tkn} = RandFr()$

$CM_{asset,tkn} = value \cdot G_{cy} + r_{tkn} \cdot G_r$

$Ticket$:

$ticket = (value, Catetory)$

$G_{cy} = Ecc(Currency)$

$r_{tkn} = RandFr()$

$CM_{asset,tkn} = value \cdot G_{cy} + r_{tkn} \cdot G_r$

$Balance$:

$$r_{balance} = \sum_{i=0}^{n} r_{in} - \sum_{i=0}^{m} r_{out}$$

$CB = r_{balance} \cdot G_r$

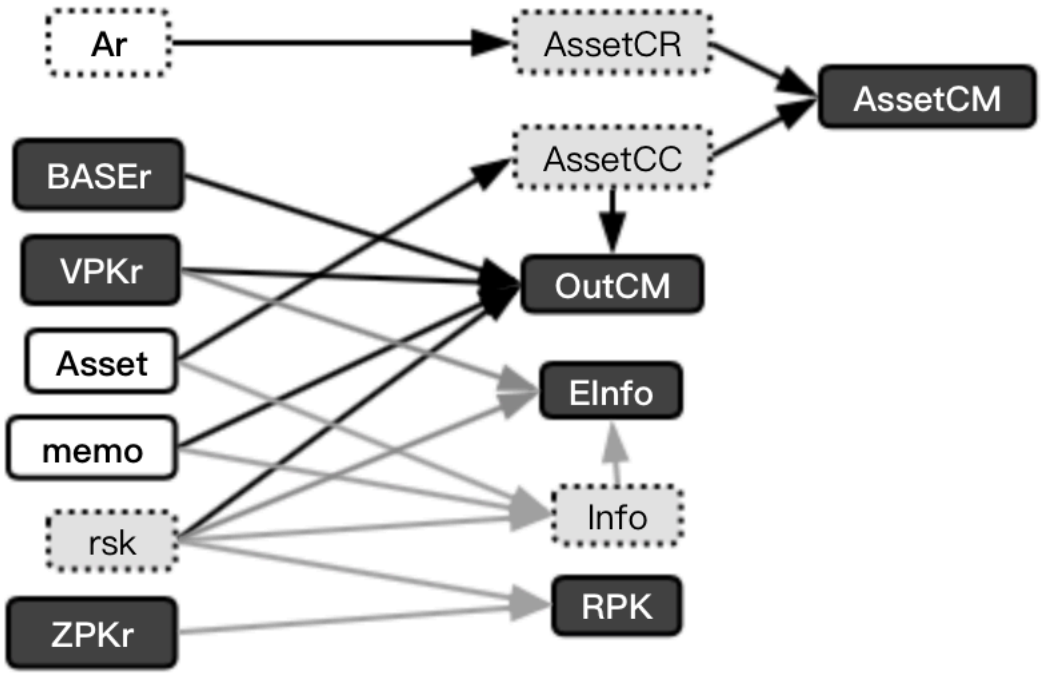
$sign_{balance} = Sign(G_r, H_{for\_o}, r_{balance})$

$check_{sign} : Verify(G_r, CB, H_{for\_o}, sign_{balance})$

$$check_{balance}: \sum_{i=0}^{n} CM_{asset,in} - \sum_{i=0}^{n} CM_{asset,out} == CM_{asset,balance} + CB$$

不管是用户账户还是智能合约账户，其下都具有管理无限种类资产的属性，除了交易费用结算采用SERO币以外，每一种资产都具有跟SERO本身等同的交易特征，除SERO币之外，其余的资产可以由智能合约产生。每种资产在产生的同时，可以赋予一个最长32 byte长度的名称(token name)，用于助记，这些名称也是不允许重复使用的。在账户进行余额查询或者转账操作的时候，可以指定资产类型。

输出系统(Output construct)



$$ar = RandFr()$$

$$rsk = RandFr()$$

$$CR_{asset} = ar \cdot G_{cr}$$

$$CC_{asset} = asset \cdot G_{cc}$$

$$CM_{asset} = CR_{asset} + CC_{asset}$$

$$CM_{out} = Hash_p(CC_{asset}, BASE_r, VPK_r, memo, rsk)$$

$$Info = Append(asset, memo, rsk)$$

$$EInfo = Enc_e(Info, rsk)$$

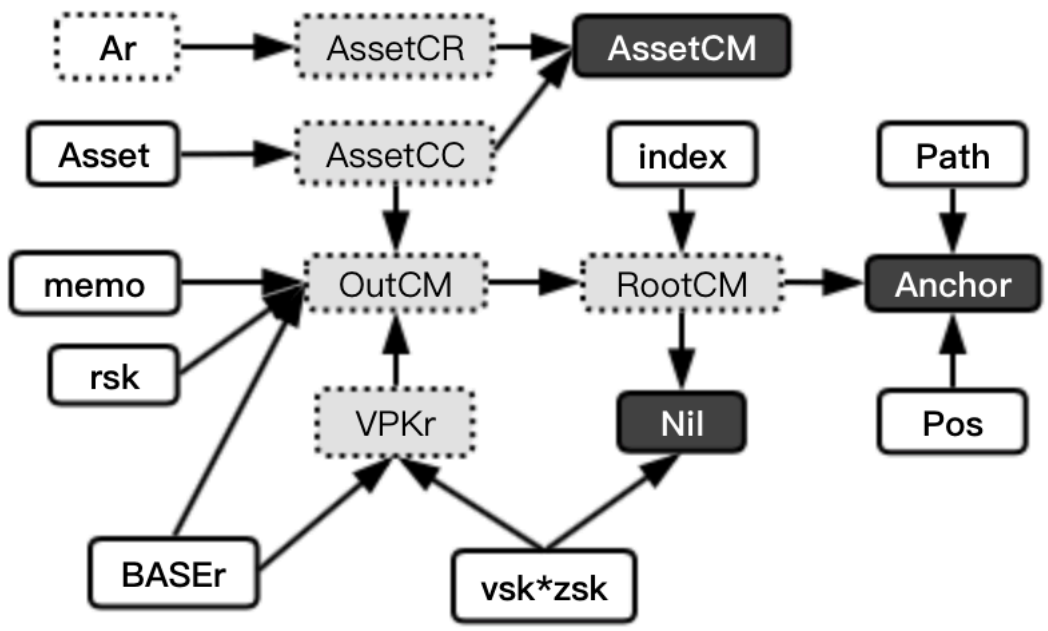
$$RPK = rsk \cdot VPKr$$

$$Inputs = (CM_{asset}, CM_{out}, EInfo, PKr, RPK)$$

$$Vars = (ar, asset, memo, ZPK, rsk, CR, CC)$$

$$Proof = Prove(Inputs, Vars, CIRCUIT_{output})$$

输入系统(Input construct)



$$CM_{auth} = Hash_{pederson}(index, CM_{out})$$

$$Anchor = MerkleRoot(index, CM_{auth}, Path)$$

$$Nil = zvsk \cdot CM_{auth}$$

$$Til = vsk \cdot CM_{auth}$$

$$Inputs = (CM_{asset}, Anchor, Nil)$$

$$Vars = ([the\ rest]\dots)$$

$$Proof = Prove(Inputs, Vars, CIRCUIT_{input})$$

CM_{auth}是由UTXO序列组成的Merkle树的叶子节点的值； $Anchor$是当前Merkle树的根，用于定位输入数据；$Path$和Pos是从CM_{auth}到$Anchor$的认证路径；Nil是一个32位的hash串，用于作废UTXO中的OUT；Til是用来追踪交易输入用的32位的hash串；CM_{out}是交易输出的资产承诺；CM_{in}是交易输入的资产承诺。

License系统(License System)

$$LICENSE:$$

$$Inputs = (ZPK, prop)$$

$$sk_{license} = (sk_{zpk}, sk_{prop})$$

$$PK_{lic} = (PK_{zpk}, PK_{prop}) = (sk_{zpk} \cdot G_{lic}, sk_{prop} \cdot G_{lic})$$

$$r_{lic} = RandFr()$$

$$R_{lic} = r_{lic} \cdot G_{lic}$$

$$S_{lic} = r_{lic} + sk_{zpk} * Hash(ZPK) + sk_{prop} * prop$$

$$LIC = (prop, R_{lic}, S_{lic})$$

$$PROVE:$$

$$R + Hash(ZPK) \cdot PK_{zpk} + prop \cdot PK_{prop} = s_{lic} \cdot G_{lic}$$

在SERO的Alpha和Beta网络中，为了确保网络初期健康发展，保证共识的健壮性和系统更新的及时性，SERO项目组有必要协调各个矿工节点。 因此，有挖矿需求的测试人员需要向SERO研发团队申请挖矿license。 除挖矿外，其他功能的测试不需要license。在尽可能不泄露矿工身份的前提下，区块会暴露license中的部分属性，这部分属性能够被SERO社区监管。在Beta网络初期，当出现网络被攻击并且发生重大危机的时候，SERO团队会通过社区投票的方式，在社区许可和监管的前提下，采用非常规手段抵抗攻击，保障社区成员的财产安全。license功能会在BetaNet上线半年后移除。

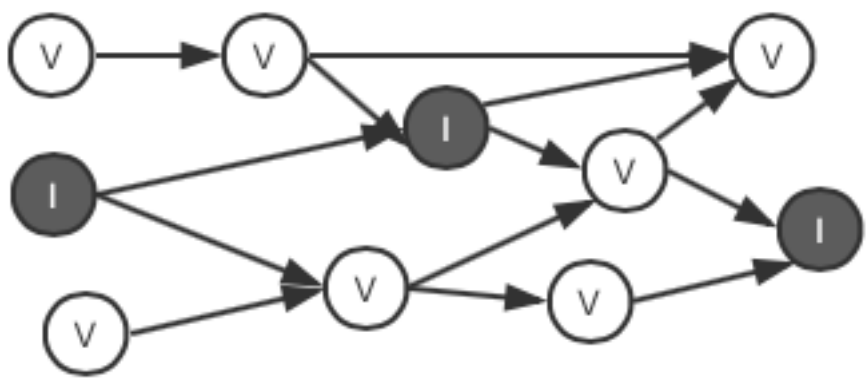
见证系统(Witness System)

SERO协议采用非交互零知识证明（NIZK），在生成交易的时候，需要提供资产来源的见证信息，每个节点会根据这些见证信息进行验证。因此，SERO会采用Merkle树维护一个记录状态变更的见证系统，系统在节点提供验证功能，在钱包端提供认证所需的信息。

$$ROOT = MerkleRoot(POSITION, LEAF, PATH)$$

$ROOT$是当前Merkle树的根，$LEAF$是第$POSITION$片叶子，$PATH$是$LEAF$到$ROOT$的证明路径。

证明系统(Proof System)



SERO的证明系统包含一个基于有向无环图的计算电路，用来描述SERO每笔交易的内部约束，包括各种资产类型的输入输出平衡、公私钥验证、承诺的有效性、见证的有效性等环节。装载好数据的电路可以通过非交互零知识证明(NIZK)生成一个Proof，通过提交这个Proof，可以在隐藏大量细节信息的情况下，让节点对电路中装载的各种参数和约束进行验证。

$$Inputs = (I_0, I_1, \ldots, I_n)$$
$$Vars = (V_0, V_1, \ldots, V_m)$$
$$Proof = Prove(Inputs, Vars, CIRCUIT)$$
$$Check : Verify(Inputs, Proof, CIRCUIT)$$

I_i是交易的公开数据，V_i是交易的隐私数据。所有变量参与构建$CIRCUIT$，证明过程采用$Inputs$、$Vars$、$CIRCUIT$生成$Proof$。然后在交易中携带$Inputs$、$Proof$，验证过程通过$Inputs$和$CIRCUIT$、$Proof$进行校验。

执行步骤(Process Step)

1. 计算(Compute)，用户采用账户、资产、见证系统提供的信息，并根据当前所需的计算，提供输入数据，然后在链下运行计算规则得到结果。

$$RESULT = COMPUTE(METHOD, ACCOUNT, DATA, WITNESS)$$

2. 证明(Prove)，用户用计算步骤得到的结果$RESULT$和随机数 r 一起封装成交易STX，并提交给节点。STX包含校验数据C_i，结果编码数据E_i和证明数据P_i。

$$STX = PROVE(RESULT, r)$$
$$STX = ((C_0, C_1, \ldots, C_n), (E_0, E_1, \ldots, E_m), (P_1, P_2, \ldots, P_m))$$

3. 验证(Verify)，节点在收到交易STX之后，将C_i在见证系统和证明系统中进行确认。验证通过后，节点接受STX。

$$ret_i = VERIFY_i(C_i)$$
$$Check = ret_0 \,\&\, ret_1 \ldots \&\, ret_n$$

4. 确认(Confirm)，资产接受方在同步到得到验证的交易STX之后，利用自己的私钥将密文E_i解出生成明文D_i, 并将明文D_i和证明P_i输入到证明系统中进行校验，成功则说明交易是真实的。真实的交易如果被n个区块进行了确认，那么交易接收方可以认为这笔交易已经确认。

$$D_i = FETCH_i(E_i, ACCOUNT)$$
$$ret_i = CONFIRM_i(D_i, P_i)$$

$$Check = ret_0 \,\&\, ret_1 \ldots \&\, ret_m$$

要说明的是，SERO的执行步骤是开放式的，也就是说这样的步骤和参数的抽象描述，可以支持“实现方案”一节中所描述的一到三期的新增功能，在后续升级时对代码结构的调整最小。

通用隐私交易

在SERO内部，普通交易中的数据都是加密的，非交易双方不能得知来源、去向、资产种类、金额等细节。系统在交易处理时并不区分智能合约产生的资产和SERO本身的资产。

线上智能合约

SERO的通用智能合约可以进行公开计算，制定对各种资产的统计方案、处置规则、公示规则，但输入输出信息都必须通过暂存地址与用户的真实身份隔离。

SERO智能合约兼容以太坊智能合约指令，也就是说以太坊大部分的智能合约可以不修改就在SERO上运行。

线上隐私资产

智能合约通过调用线上隐私资产发行方法发行的资产，资产总数量公开，并具有与SERO币等同的交易属性，可以通过通用隐私交易进行处理。

线下隐私资产

用户通过调用线下隐私资产发行方法发行的资产，资产总数量不公开，具有与SERO币等同的交易属性，可以通过通用隐私交易进行处理。

线下智能合约

SERO的线下智能合约只在用户机器上运行，计算规则只对部分用户可见，共识对运行结果的正确性进行验证。

3.4 关于非交互式零知识证明(NIZK)的性能优化

对于采用非交互式零知识证明（NIZK）方案的区块链系统，目前最大的应用瓶颈就是交易时生成证明（Proofs）的时间太长，SERO系统的零知识证明模块Super-ZK，针对这一瓶颈，做了以下突破性创新。

1、当前我们采用zk-SNARKs框架生成NIZK，采用其中的ALT_BN128曲线和Groth16预处理过程，这个过程比PGHR13预处理方案减少1/3的运算时间。虽然zk-SNARKs框架需要信用安装过程，但SERO的实现方式中不会动态构造计算电路，因此，在当前所有场景下，zk-SNARKs框架能满足SERO的需求。

2、我们创新性的开发出一种Twisted Edwards曲线，以取代SHA256来生成公钥，采用ECC Hash进行Merkle树的生成，这样可以提升4倍以上交易生成速度。

3、SERO采用单路输入和输出结构，每个描述之间采用资产通道进行链接，这样的电路构造更加模块化，在多核CPU情况下，并行执行效率获得3倍的提升。

4、Super-ZK的部分代码由汇编语言进行编写，优化了资源分配等工程结构，使其具有更高的代码执行效率。

综合以上优化，在交易证明生成速度上，我们相比于直接使用zk-SNARKs的其他区块链系统，有一个数量级的速度提高，极大的提高了NIZK系统的适用性。

3.5 SERO支持智能合约发行和操作匿名资产原理

区块链账本的UXTO和ACCOUNT模式

区块链是分布式账本，账本的最小单位是记录，每一笔账记录资产的流入和流出，根据资产流出记录方式不同，有两种不同的记账实现，分别为UTXO模式和ACCOUNT模式，这两种模式分别对应比特币和以太坊的模式。

UTXO的特点是：

A. UTXO模式每笔交易是相互独立的，这意味着只要能处理好双花的问题，一个账户下的交易都可以进行并行处理，能充分利用多核CPU的能力。

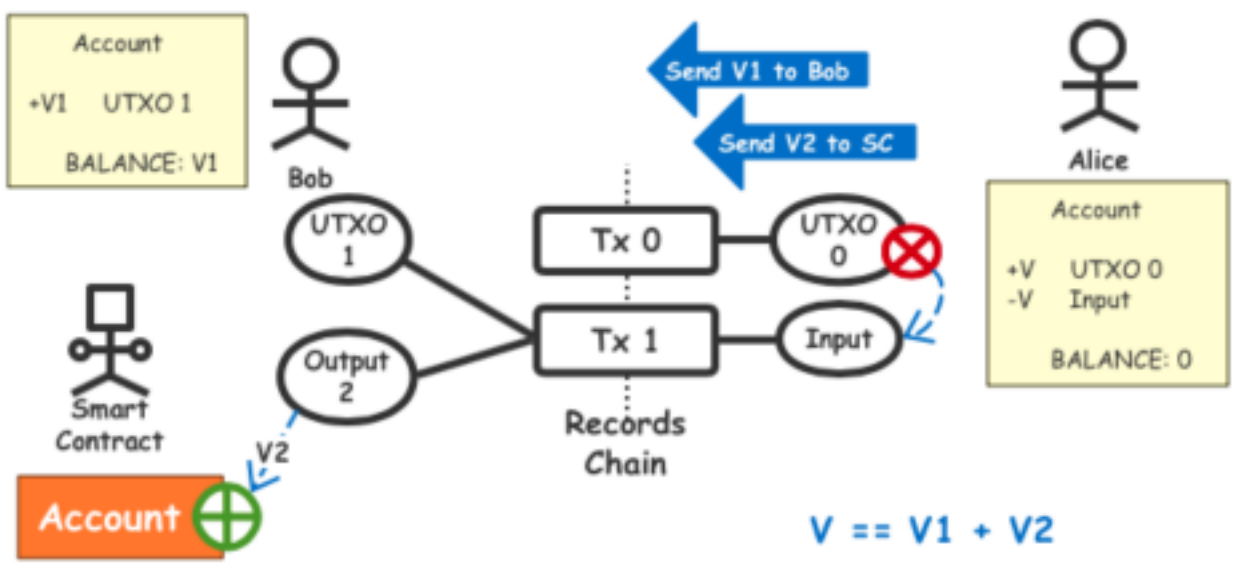
B. UTXO本质上来说是基于历史的记录形式，即是过程，也是结果，因此在一些需要生成见证证明的应用场合下，具有非常大的优势，这也是为什么现在的匿名币区块链系统基本都是UTXO模式。

ACCOUNT模式的特点是：

A. ACCOUNT模式直接增减一个独立账户的资产，只需要一个记录就可以增减一个账户的任意数量的资产。因此，生成记录大小比同样情况下UTXO生成的记录要小很多。

B. ACCOUNT模式本质上是基于状态的，输入和输出是过程，account是结果，因此它天然就很容易把图灵机引入进来，这也是为什么支持图灵完备智能合约的区块链系统多采用ACCOUNT模式的原因。

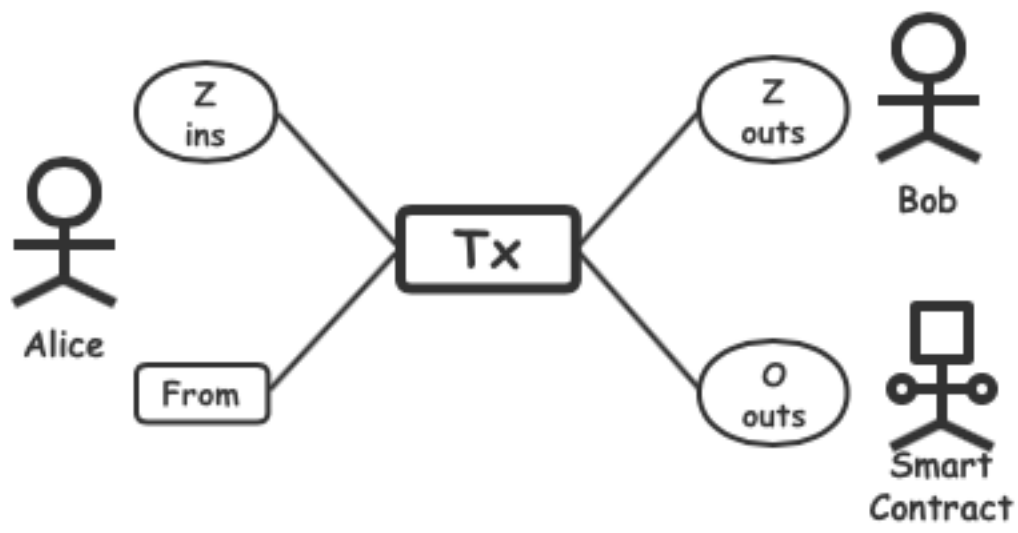
SERO独特的混合模式



SERO将UTXO和ACCOUNT模式混合应用，在隐私保护的计算层采用UTXO模式，同时可以映射逻辑上等价的ACCOUNT模式以支持图灵完备的智能合约虚拟机的运行。SERO通过交易、共识、以及Pedersen Commitment算法，将两种模式无缝结合到一起，使智能合约能发挥出令人惊讶的能力。

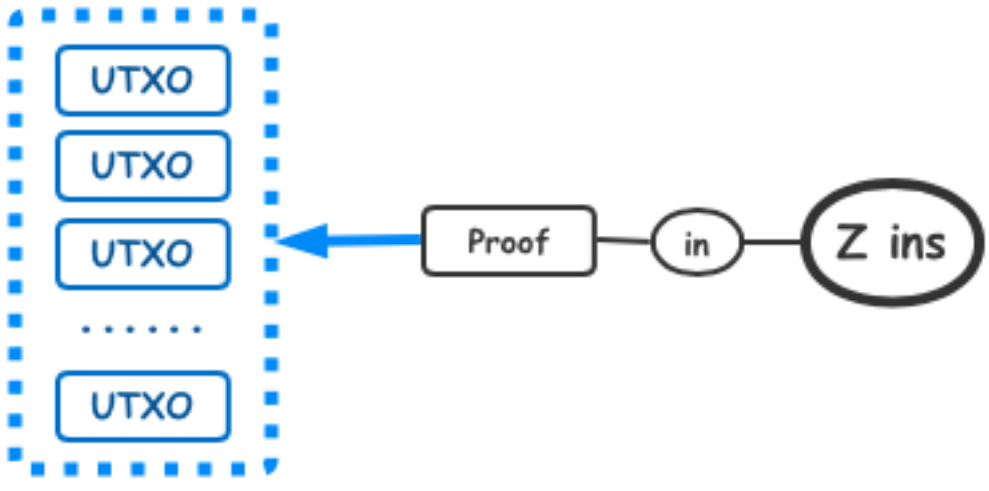
支持智能合约匿名交易的结构

A、交易



SERO的匿名交易Tx拥有一个匿名的输入集合“Z ins”，一个匿名的输出集合“Z outs”，一个普通的输出集合“O outs”和一个名为“From”的暂存地址。“Z ins”是完全匿名的，让第三方观察者无法得知来源和内容，“Z outs”是完全匿名的UTXO，只有接受者能查看和使用它的内容，“O outs”携带的内容是非隐藏的，它指向的接受者有两种情况：一种是指向智能合约地址，一种是指向一个暂存地址。From代表交易的发送者，同样也是一个暂存地址。因此整个Tx无法让人确定真实的用户是谁，其中携带的资产信息也被最大程度隐藏起来。

B、“Z ins”输入



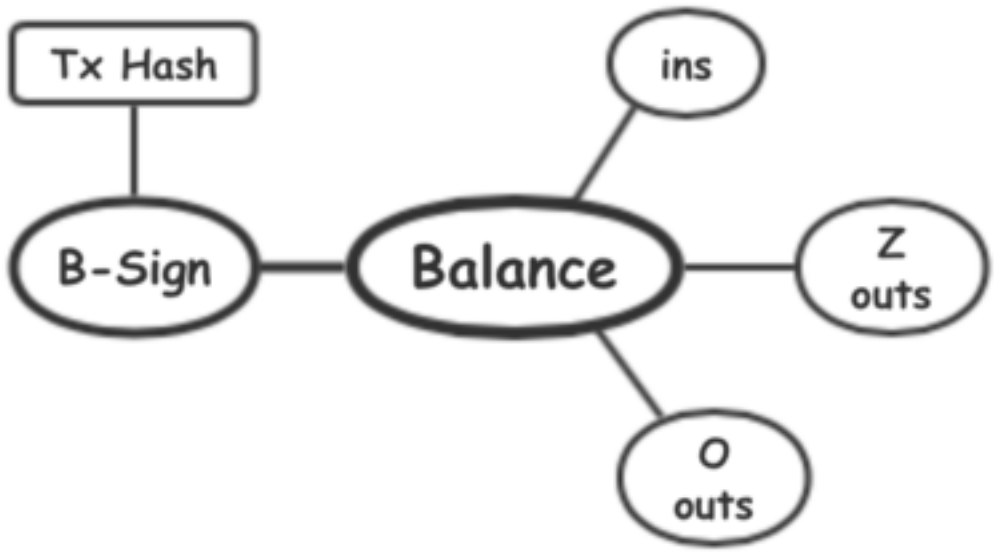
在SERO交易的输入集合“Z ins”中，每个输入都是匿名的，包括来源“UTXO”的Id以及其携带的资产信息。每个输入都通过零知识证明生成的Proofs，指向一个被隐藏在巨大UTXO序列中的特定某个UTXO，这个序列是SERO历史的一部分，所有细节都被Proofs隐藏起来，验证者在不知细节的情况下，通过Proofs能确认这个输入是否合法。

C、“Z outs”输出和“O outs”输出

“Z out”指向暂存地址PKr，暂存地址只有接受者能解密出身份。由于每个暂存地址都不一样，所以没有第三方能识别“Z out”的指向。“Z out”还携带了资产的加密信息“Encrypt Info”，只有持有接受者私钥的人才能解密这些信息。而OutCM是输出承诺，只有交易双方才能复现OutCM的计算过程。“OutCM”在证明“Z out”被“ins”引用这一过程中起到关键的作用。

“O out”指向的PKr有两种形式，一种是由智能合约发起的，指向普通账户的暂存地址。另一种是由普通账户发起的，指向智能合约的地址。由于暂存地址的随机性，第三方无法得知接受者的身份。

D、输入和输出的平衡“Balance”



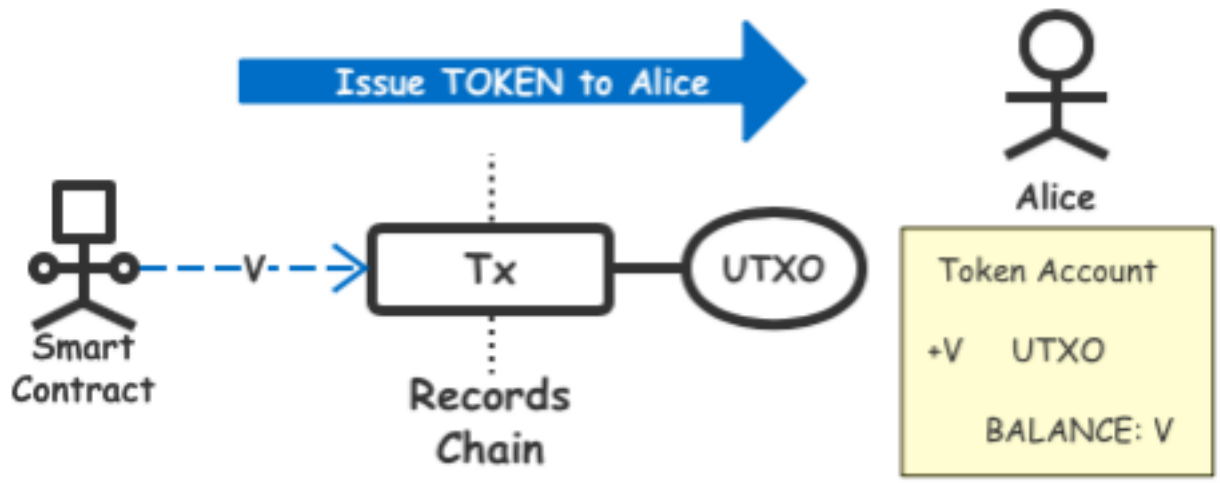
Tx将“ins”、“Z outs”、“O outs”打包到一起，我们使用Perdesen Commitment来防止恶意攻击者篡改里面的数据并确保资产的安全，它的同态加密特性使验证者在不知道信息细节的情况下，可以确认Balance一定是平衡的，即输入等于输出。

另外，为了防止恶意攻击者对“O outs”的篡改，我们使用Perdesen Commitment的随机特性，以“Balance”的随机部分对“Tx Hash”进行签名。这样，每个输入和输出都可以独立进行计算，并通过“B Sign”打包到一起。

E、交易发送者“From”

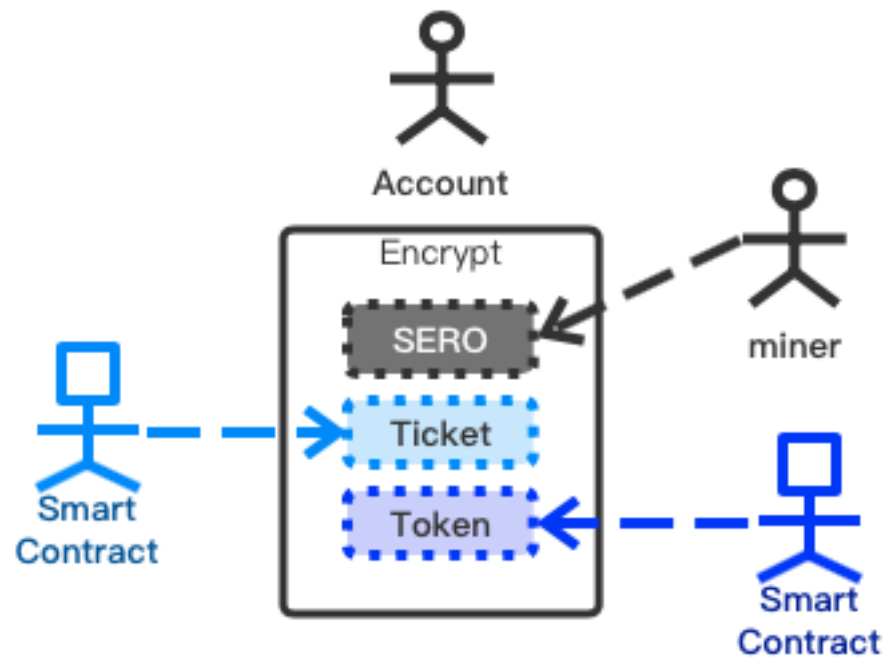
当交易的输出是指向智能合约时，某些情况下的智能合约会根据编写的规则，把资源输出到给定的账户。这时暂存地址“From”就是承接输出资源的地方。“From”在交易生成的时候就被确定，并且只使用一次，除了交易发送者外，其他人无法定位发送者的身份。

F、匿名Token的发行

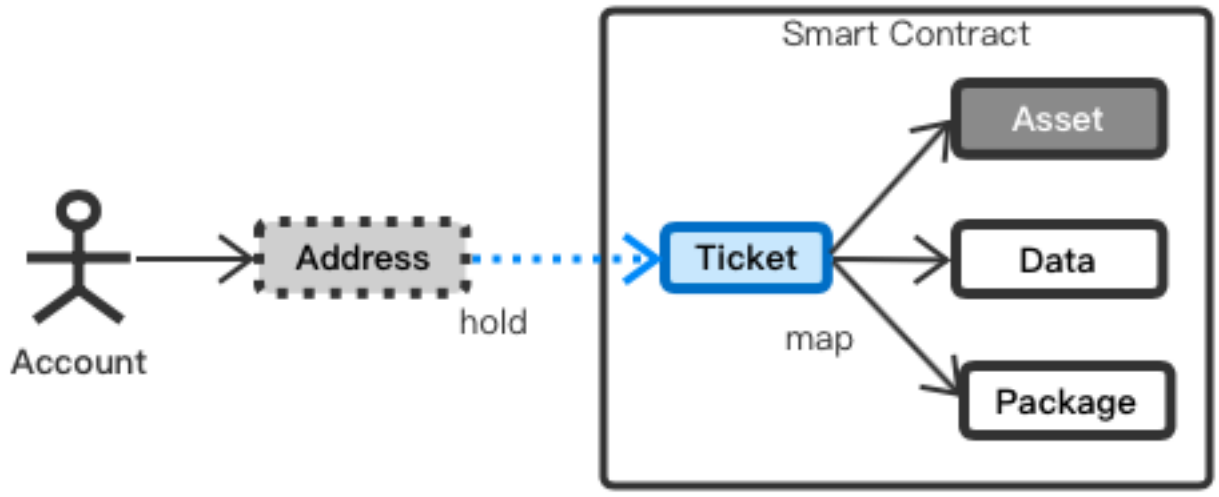


Token又被称为“同质化通证”，是SERO系统内部的一种资产形式，相同种类的Token可以任意的分割和混合。SERO系统上的Token和以太坊Token不同。SERO币作为SERO系统的第一个币种，本质上也是一种Token。对于Token资产，除了手续费规定只能以SERO币缴纳外，在SERO系统内部是同一对待的，具有相同的基于零知识证明的安全性。匿名Token可以使用SERO的智能合约任意发行，一旦匿名Token发行成功，智能合约可以将Token以普通交易的形式发送到某个账户的暂存地址PKr，这时这些被发送的Token将以UTXO的形式脱离智能合约账户，并且与SERO币一样，进入用户的个人账户中，从而被SERO的零知识证明隐私机制所保护。

G、SERO系统对非同质资产（Ticket）的支持

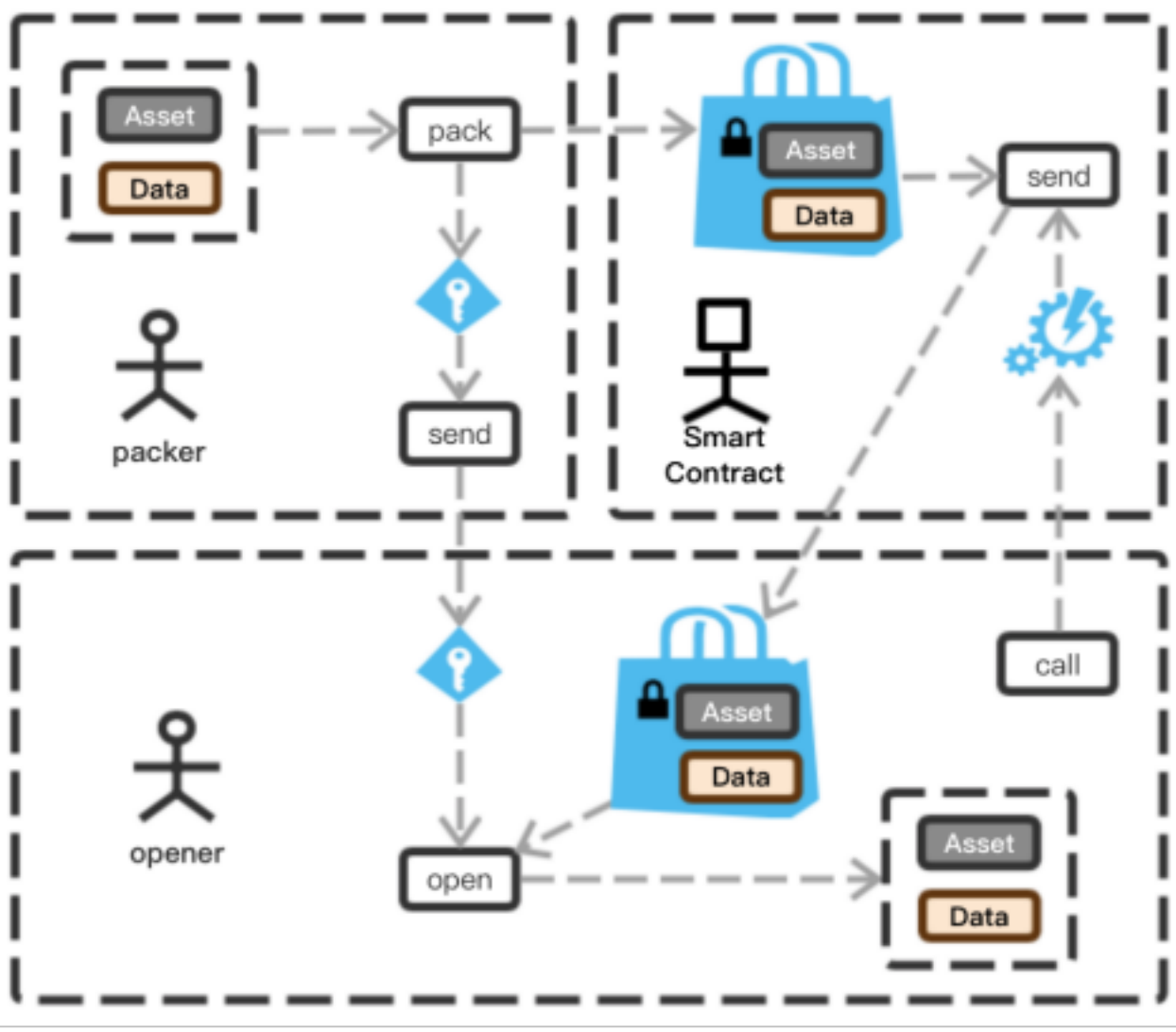


Ticket又被称为“非同质化通证”，是SERO系统内部的另一种内涵更为广泛的资产形式。Ticket和Token不同，是一种不可分割的，具有个体唯一性的通证形式。和Token一样，SERO对Ticket同样提供了匿名性的支持。当匿名Ticket发行后，智能合约将表现为ID形式的Ticket的以普通交易的形式发送到某个账户的暂存地址PKr，这些Ticket将会以UTXO的形式脱离智能合约账户，以和SERO币以及Token类似的机制，被SERO的零知识证明隐私机制所保护。



Ticket是一个256bit的数字，可以指向在智能合约中保存的复杂的数据构造，因此可以适合复杂业务场景的构建。Ticket所指向的数据结构的简明示例如上图，Asset是资产的数据结构，这个资产的数据结构可以是SERO币，Token或者是Ticket，因为Ticket的对数据的指向性，所以这种结构可以支持无限的嵌套，组成符合业务需求复杂的资产结构。Data可以保存除资产外的其它数据结构编码而成的数据，这个数据代表的数据结构也是可以嵌套的。Package保存的是用户用一个密钥编码后的资产或数据。利用Ticket功能，开发者完全可以把加密猫这类复杂的游戏应用改造成匿名版本的实现。

H、SERO系统对加密的资产或数据包（Package）的支持



在以数据为中心的应用中，这些数据包括时间戳、高价值的数据存储、各类证明数据或密码串、资产数据等等，比如类似医疗数据等高度隐私性的数据。这些应用如果用区块链来实现，并由智能合约来输入和输出，会遇到了明文数据的暴露问题。SERO也提供了相应的数据保护技术，让这些明文数据的暴露由用户自己来控制，这种技术叫Package。当前版本的Package应用了对称性加密技术ChaCha20，加解密速度很快并且非常安全。用户可以在客户端打包Package，并得到相应的密钥，打包之后，这个Package可以进行匿名转移，或者输入到智能合约中进行相应的逻辑操作，在此过程中，这个加密Package里的内容都是不可被破解的。当需要解密时，用户可以根据自己的情况，私下把密钥转移给关联方，让关联方使用密钥解密出相关的资产和数据。

I、总结

SERO币、Token、Ticket、Pagkage这四种类型的资产共同组成了SERO系统匿名资产的生态，这几种资产类型都在一套编码体系内完美的融合，结合SERO系统的图灵完备的智能合约对这些资产的编程，开发者可以开创性得在链上实现在之前系统上无法实现的各种隐私保护相关的DApp，适用于各类隐私保护领域的业务需求的实施。

3.6 SERO面向的场景

隐私保护是现实世界中个人与组织都存在的强烈需求。SERO支持图灵完备的智能合约和各类相关隐私组件，能支持不同经济生态的拓展。由SERO系统开始，匿名资产的发行和掌控权将不再为少数对密码学有深厚造诣的极客组织所独享，普通开发者，只要有相关业务需求，都可以在SERO链上发行自己的匿名资产，建立自己的隐私生态，这极大拓展了区块链隐私保护相关技术的适用范围。下面列举几个典型的使用场景：

A、供应链体系

区块链可以解决供应链体系上下游交易凭证和溯源的难题，简化了供应链中心企业管理的难度并给上下游企业的融资提供了相应的解决方案。但是，价格、货物等敏感数据，上链的话又面临泄露商业机密的难题。而利用SERO系统，可以完全解决商业机密暴露的难题，同时，又让参与各方享受到应用区块链系统所带来效益提升。

B、医疗健康

在医疗健康相关行业，数据隐私体现于方方面面，从个人病例到医疗记录，面向多角色的隐私保护和授权机制需要十分灵活和安全的隐私保护能力，涉及到医院、患者、保险公司、医药公司等，数据隐私的保护和限制授权使用显得尤为重要。SERO系统，可以解决患者和医院面临隐私问题，同时也为保险公司和医药公司安全合规并且在患者许可的情况下使用相关数据打开了通道。

C、在线竞拍

在诸多追求公平的在线竞拍业务中，出价的私密性是非常重要的，但在利益的驱使下往往难以做到，而SERO可以提供一个完全安全、独立、公平的竞价环境。

D、在线博彩相关行业

在线博彩业的发展一直以来都受到中心化机制的制约，在这个巨大的现金流行业中，非常需要一个能够提供多人出价、支付、结算的去中心化智能合约体系，SERO系统能完全支持这类业务。

E、游戏

大型的游戏往往需要一个易于流通、交易和结算的货币体系，并能基于智能合约发行和流通，同时还要兼顾交易的隐私保护。而目前SERO是唯一能做到多货币体系能基于同一智能合约体系发行和流通，且兼顾交易隐私的技术方案。

还有更多的涉及资产数字化，又涉及数字资产隐私敏感的行业，如保险行业、数字贵金属交易、期货交易、数字资产交易（如征信和知识产权等）、信贷行业等。在这些领域，SERO系统都大有用武之地！

3.7 未来计划

链下计算和同态加密智能合约

事实上对智能合约的同态加密已经进入到实质开发阶段，并计划于2019.3发布到2.0版本的SERO平台上。目前我们已经找到了一种通过链上和链下计算，兼顾数据安全（可以面向计算者完全隔离敏感数据的机制）与性能的方法，并计划于6个月内完成这项工作。

钱包和其它生态应用

SERO的去中心化钱包应用目前同样正在开发当中，并计划于2019.3前正式发布，由于SERO支持开发者自己发行Token的特性，SERO的钱包将会支持SERO自己的Token以及所有开发者基于SERO发行的Token所对应加密货币资产的管理。

最新共识机制

我们会在1年内的某个版本发布新的共识机制SE-Random，结合了最新的PBFT理论和VRF算法设计的一种可以相对兼顾公平和效率的共识机制。

隐私三剑客

SERO有两个兄弟，分别是异形协议 （Alien Protocol）和卡斯特罗协议（Castrol Protocol），前者提供一种分布式的DNS系统，通过自动寻址的方式实现网络的稳定运行和信息传输，后者则对节点的IP地址实现加密隐私保护，三位一体形成完整的去中心化应用隐私保护方案。

安全多方计算

在许多情况下，数据证明需要结合现有的中心化的数据源，也可以成为链下数据源，当前，解决上述问题的策略是假设有可信任的服务提供者或是假设存在可信任的第三方。但是在目前多变和充满恶意的环境中，这是极具风险的，面对该问题，通用的安全多方计算问题是可解决的。

SERO未来也将考虑引入安全多方计算（SMC），从而在隐私保护的前提下实现对链外数据的广泛支持。

多链体系

多链体系是SERO可扩展性解决方案。SERO将采用类似以太坊Plasma的机制进行基于多链体系的横向的性能扩容。类似Plasma的多链并行计算机制，可使SERO的每秒状态更新达到极高水平（可能会有数十亿）。从而使SERO在性能上取代当前中心化集群的能力，让SERO具有处理全球的各类隐私相关去中心化应用的前景。

第四章 链的基础框架

除了隐私保护的机制之外，链基础架构同样需要具备足够强大的可扩展性，这对于构建一个实用的应用平台显得十分重要，SERO会引入以下技术来对链的底层架构进行增强：

- 优化共识 – 使用一种全新的共识机制**SE-Random**，它结合了最新的PBFT理论和VRF算法设计的一种可以相对兼顾公平和效率的共识机制。
- Plasma – 是一种实现区块链扩容计算的方式，在plasma中，众多区块链组合成树形结构，共同参与计算，从而实现区块链的横向扩展。
- 更为强大的虚拟机——不仅满足EVM的兼容性，而且有充分的扩展性，并且要有底层指令的基础来满足性能的需求。
- 以下会重点阐述部分技术的具体实现。

4.1 共识机制

SERO在研究各类共识的基础上，提出了自己的主链共识引擎SE-Random。SE-Random共识引擎的设计思路受到最新一代共识研究Algorand和Ourboros的启发，只需要验证节点很少的计算开销，整个区块链网络产生分叉概率极小，并能实现近乎无限的扩展性。

下面描述一下SE-Random共识的细节。

SE-Random使用拜占庭协议BA*（Byzantine Agreement）在一组交易中达成共识。为了扩展性，SE-Random使用一种随机算法筛选出一批用户，允许用户自己私下检查是否被选中，并参与BA*协议中共识的达成。在此算法下，随着用户量的增多，整个BA*共识系统不会变慢。

VRF算法的使用

SE-Random共识引擎基于VRF（Verifiable Random Function）算法作为随机验证节点选择基础。VRF是随机生成函数，而且这个函数是可验证的。即同一把私钥对同样的信息进行签名，只有一个合法签名可以通过验证，这个有别于普通的非对称加密算法。

VRF的具体操作流程是：

1. 证明者生成一对密钥，PUB_KEY和PRI_KEY。PRI_KEY是私钥，PUB_KEY是配对的公钥。

2. 证明者输出随机结果 $result = VRF\_Hash(PRI\_KEY, info)$

3. 证明者输出随机证明 $proof = VRF\_Proof(PRI\_KEY, info)$

4. 证明者把随机结果和随机证明提交给验证者。验证者需验证result和proof是否匹配，若匹配，进入下一步。

5. 证明者把PUB_KEY和$info$提交给验证者，验证者计算$VRF_Verify(PUB_KEY, info, proof)$结果是否为$TRUE$，是$TRUE$的话即验证通过。

6. 验证通过即可推导出$info$和$result$是否匹配，即证明验证者给出的材料是正确的。在整个过程中验证者没有拿到证明者的私钥PRI_KEY。

随机种子（Seed）生成

在SE-Random的一些地方的随机算法会用到种子（seed），比如SE-Random的加密抽签中，需要随机选择并公开的种子。这个seed既要让参与节点知晓，又不能被对手控制。SE-Random第r回合产生的seed是由上一回合r-1的seed通过VRF来确定。这个种子和相应的VRF证明被包含在每个被提出的块中，一旦SE-Random在r-1轮的块上达成一致，当r轮开始之后，每个人都知道当前轮的伪随机的seedr 。初始的seed0的值是由初始参与者们一起用多个节点进行计算，得到的一个绝对无法预测的随机seed。这样，seed不会被“破坏者”预测，也不会被操纵。

通过VRF算法进行加密抽签选出验证者的方法

SE-Random用加密抽签方法来根据每个用户的权重来选择用户的随机子集。系统将固定单位数量的SERO币设为一个筛选候选单位S，并规定每个节点有限定数量的SERO币w作为筛

选计算，所有候选单位的总权重是$W=\sum_i \frac{w_i}{s}$ 。并且如果节点i拥有j个筛选单位数量的SERO币，则节点i可以以j个不同的子节点的身份参与抽签筛选。抽签算法的随机性来源于前面提到的随机种子。在BA*的每次循环中，SE-Random基于当前seed构建一个VRF，VRF的私钥只能由节点自己知道。每个节点用自己的私钥运行系统公布的随机算法进行抽签。系统按照节点持有的不超过限定阈值SERO币的比例选择验证节点。

SE-Random需要指定阈值，用以选择验证节点的预期数量。这个预期数量满足概率$p=w/W$。在W（总节点权重）选择子验证节点的概率满足二项分布：

$$B(k;W,p)=\binom{W}{K}p^k(1-p)^{w-k}, where \sum_{k=0}^{W} B(k;W;p)=1$$

当前验证节点（包含子验证节点）的选择数量的确定方式也是由抽签算法确定的。抽签算法将区间[0,1)划分为连续区间的形式：

$$\mathbf{I}^j=\left[\sum_{k=0}^{j} B(k;w,p), \sum_{k=0}^{j+1} B(k;w,p)\right) for\ j\in\{0,1,...,w\}$$

如果散列的比特长度为hashlen，如果$hash/2^{hashlen}$在间隔$\mathbf{I}^j$中，则节点就有j个选定的验证子节点。选择的验证节点数目可以使用π进行VRF公开验证。

此加密抽签的方法的特性为：

1、验证节点根据他们持有SERO币的权重随机选出N个验证子节点

2、不知道节点i私钥的破坏者无法知道i是否被选中，以及选出多少个子验证节点。

在随机选出的验证者节点中进行BA*共识计算

验证节点（包括子验证节点）在秘密的情况下获知自己被选中，但他们只有公布凭证才能证明自己的验证者资格。对于每一个选中的节点，使用自己的私钥对seed进行签名，并输入哈希函数后得到自己的凭证。哈希函数的性质表明凭证是一个随机的长度为256的字符串，不同节点的凭证不会相同，并且凭证字符串的分布是均匀的。用同样的方式选出一批候选领导节点，把候选领导节点的凭证按照字典顺序进行排列，排序中最小的候选领导节点被选为领导节点，即领导节点是通过候选领导节点集合随机的公共选举产生。

验证节点和领导节点一起参与拜占庭协议BA*的运算，在BA*的每一个阶段和步骤里，节点都通过私人和非互动的方式来独立确定自己是否被选择在当前步骤的委员会中。BA*是一个两个阶段的投票机制。第一阶段，验证节点对收到的候选区块进行分级共识，选取验证共识最多的候选区块。第二阶段，对第一阶段筛选出的候选区块进行二元拜占庭判断。BA*共识要保证参与共识的诚实节点大于2/3，如果随机选出的集合不能满足该条件，那么需要进行多次随机选举，只要有一次参与共识的诚实节点大于2/3，就能达成共识。BA*共识的每个步骤的验证节点并行指定或抽签筛选出来用来加快共识确认速度。

BA*共识计算的步骤

BA*的每一步都要销毁当前步骤临时密钥，步骤简述如下：

1. 生成区块（Step1）

1）节点检查自己是不是领导节点 B_i^r 。

2）生成第一步的消息 $m_i^{r,1}=\left(B_i^r, ESG_i\left(H\left(B_i^r\right)\right), \sigma_i^{r,1}\right)$

3）广播 B_i^r 和 $m^{r,1}$

其中 $m_i^{r,s}$ 是节点i在 (r,s) 广播的消息； B_i^r 是第r轮里节点i生成的区块； ESG_i 是指用当前 (r,s) 的临时密钥来签名信息；H是哈希计算； $\sigma_i^{r,s}$ 是指I的签名 $SIG_i(r,s,Q^{r-1})$ ，用来证明i存在于 (r,s) 的验证节点集合里。

2. 分级共识协议

这个协议将在任意一个块上达成一致的问题转化为在的两个值上达成一致，这两个值是最后确定特定块的散列或者空块的散列的依据，总共分为3个步骤，我们会在后面的技术黄皮书中详细说明。大体来说判断消息中是否有超过2/3的 $\left(ESG_j\left(V^{'}\right), \sigma_j^{r,2}\right)$ 并且相同，如果有，则广播此特定区块，如果没有，则广播空块，此消息用于后继二元拜占庭判断。

3. 二元拜占庭判断

在这里验证节点统计判断分级共识协议发出的值。二元拜占庭判断是一个三步的循环，验证节点会不断的对收到的历史进行检查，看是否达到了有两种结束条件，即区块合法或者区块不合法是否达到2/3的投票总数；如果区块不合法，共识系统会判断并生成一个空区块。为了预防无限循环的情况发生，我们会设定一个最大总循环数m，如达到m后还没判定出是否符合一个结束条件，共识系统会临时生成暂定的共识，并在后续过程中（后面几轮）形成最终共识，并确认这些较早的交易。

SE-Random共识会适应网络弱同步情况下的共识判定。在网络强情况下不会造成区块分叉，在网络弱同步情况下，会临时做出暂定共识并在网络强同步恢复后达到最终共识。SE-random可以防范女巫攻击、自私挖矿攻击、Nothing-at-Stake攻击、远程攻击等各类攻击方式。即使SERO链的用户扩散到亿级以上的节点，SE-Random共识也可借助VRF机制快速达成全网一致的拜占庭共识。

4.2 扩容机制

Plasma是一个激励，和强制智能合约执行的框架。可以扩容达到每秒大量的状态更新（能达到每秒10亿级），在区块链上能支持全球范围内的大量的去中心化金融应用。这些智能合约通过网络交易手续费用于激励持续的自动化运作，最终依赖于底层的区块链来强制交易状态的锁定。

Plasma由两个核心部分构成：重组所有区块链计算为一组MapReduce函数，和一个可选的方法，在现存的区块链上，以不鼓励区块扣留的Nakamoto共识原则，来实现一个Pos的代币押金机制。

这种构建通过在主链上编写智能合约，使用欺诈证明，可以在主链上强制状态的锁定。Plasma将区块链编组为一个树形的分层结构，将每一个区块链视为一个独立的分支，强制将整个区块链的历史，和可MapReduce的计算提交到Merkle证明。通过主链强制将某个链的帐本信息打包到子区块链中，这个链将通过最低的信任达到扩容的需求。

围绕全局强制非全局数据的数据可用性，区块扣留攻击是是一个非常复杂的问题。Plasms通过对有问题链的退出机制来缓解了这个问题，同时也创建了一个激励和持续的强制的执行数据的正确性机制。

仅仅通过周期性的将正常状态的Merkle证明广播到主链，这将允许不可思议的扩展性，降低交易成本和计算量。Plasma支持了大规模去中心化应用的持续运行。额外的，重要的可扩展性是通过减少单次花费的资金表达方式为一个位图中的一个位来实现，这样，一个交易和一个签名代表一个与多方的交易聚合。Plasma将这与一个MapReduce框架结合，同时使用含押金的智能合约来构建可扩展的计算强制性。

这种构建方式允许让外部的参与方持有资金，并根据自己的行为计算合约，类似于一个矿工，但是Plasma是运行于一个已存在的区块链上，由此大家不用在每次状态更新时在主链上创建对应的交易（即使包括添加新用户的账本），而只需要将合并后的状态变化这样的少量信息写到链上。

SERO将采用Plasma这样的机制进行基于多链体系的横向的性能扩容。这种多链并行计算机制，可使SERO的每秒状态更新达到极高水平（可能会有数十亿）。从而使SERO在性能上获得很大提升，达到取代当前中心化集群的承载能力。

4.3 虚拟机

目前以太坊已经拥有了大量开发者，Solidity语言也已经成了智能合约开发最广泛使用的语言。因此，我们需要在SERO系统中提供EVM的兼容性。

EVM虚拟机是在以太坊的基础上发展出来的，以太坊是一个标准的区块链结构，其数据结构是单一的，因此其虚拟机在交易调用层面设计为类似数据库的ACID（Atomicity，Consistency，Isolation，Durability）特性。即在以太坊的协议中，一个智能合约的调用，可能会影响多个账户的状态变化。这些状态变化是有实时一致性的刚性事务，即这些状态变化要么同时发生，要么都不发生。但是，SERO需要考虑到未来充分的扩展性，并且要有底层指令的基础来满足性能的需求。我们将SERO链的虚拟机设计为满足BASE（Bascically Available，Soft state，Eventual consistency）理念的最终一致性方案，我们将此虚拟机称为MEVM虚拟机。

在BASE理念中，基本可用是指系统在出现不可预期的故障时，允许损失部分可用性；软状态是指允许系统中的数据存在中间状态，不过该中间状态的存在不会影响系统的整体可用性；最终一致性是指所有的数据副本，在一段时间的同步之后，最终都能够达到一致。和ACID概念的强一致性相比，BASE理念通过牺牲实时强一致性来获得可用性，但最终会达到一致状态。区块链中区块结构和各类共识算法，其本质都是符合BASE理念的，不过并不满足ACID。因此MEVM虚拟机设计为复合BASE语义是适合的，并且在此层面上相比原来的EVM的ACID设计，会克服运行性能瓶颈的这个方面的制约。

另外，Solidity语言一直被人诟病的一点是缺乏标准库的支持，比如比较两个字符串这种基本的功能，Solidity中没有标准库函数给开发者调用。类似OpenZeppelin这样的项目提供了一些标准库，但是还远远不够用。特别是SERO的区块链应用需要用到的高级的数学和密码学算法库，比如零知识证明协议、RSA公钥加密算法，奇异值分解等。MSolidity可以参考这些实现并添加更多的库，这些库采用预编译或者用Native方式实现，以减少运行消耗。

在今后的发展中，SERO体系会考虑对基于Web Assembly(WASM)的虚拟机提供支持，从而进一步提升性能，并提供对除了Solidity外用更多的语言，比如C，C++，Rust，或者Go语言编写的智能合约进行支持。随着Cardano项目组设计的IELE虚拟机的成熟，SERO体系也会考虑提供对这个虚拟机进行支持。IELE是LLVM的一个变种，有希望成为高级语言的智能合约翻译并执行的统一、低级的平台。通过IELE虚拟机，可以让SERO体系支持更多种类的高级语言。

4.4 抗量子计算

目前区块链系统上普遍使用的非对称加密签名算法，比如基于大整数因子分解难题的RSA算法和基于椭圆曲线上离散对数计算难题的ECC算法，可以被量子Shor算法将NP问题变成P问题，从而容易被破解。SERO体系会根据项目进度和量子计算机实用化的发展适时引入抗量子计算暴力破解的加密算法，比如基于格的密码系统（Lattice-based cryptography），基于编码的密码系统（code based cryptosystems）和多元密码（multivariate cryptography）等；其中基于格密码可以设计加密、签名、密钥交换等各种密码系统，是后量子密码学算法的一个重要方向。同时，我们也会对基于超特异椭圆曲线上同源问题（Isogen）、共轭搜索问题（conjugacy search problem）和辫群（Braid Groups）相关问题等设计的抗量子密码系统的前沿研究方向进行同步追踪。

第五章 激励的经济模型

传统的点对点通讯网络将焦点关注于信息传输，有点像互联网1.0时代的应用，一切都是公开和共享的，而其并没有达到区块链技术所达到的震动效应，一方面是因为缺少有效的共识机制将分散的节点协同参与工作（仅限于点和点的共识），而更重要的是因为一切人类的行为都是需要背后的经济逻辑驱动的，在缺乏有效的经济规范趋势下人类的行为只能受到社会规范约束（即出于公益性质的精神激励的驱动下的工作），这对于大部分需要共同完成的目标而言对个体是缺乏约束力的。

比特币网络通过POW（工作量证明）共识机制，并以贡献算力获得记账权从而获得比特币奖励的方式激励节点参与共识，无疑是一项了不起的设计，我们认为Token经济模型是区块链价值的核心也不为过。

然而问题在于同一种token是否能解决所有共识协同行为的激励问题？我们认为答案显然是No。现今我们发现市场上有各种流通的Token，背后的经济模型五花八门，但是缺乏统一的标准将其共识的成本与产生的共识价值关联起来，因此整个加密货币的二级市场流通规则显得相当脆弱。

以太坊基于同一种底层共识机制，允许智能合约开发者发行自己的Token，并且使用ETH作为GAS费用支付共识成本，既统一了共识成本的计量单位，又允许在相同的共识成本下，能够根据Token所用于的生态获得不同的价值输出，使用者至少能够计算最佳的投入与回报的平衡点，如今许多人诟病在以太坊上发行ERC20的代币太过容易导致鱼目混珠，却很少有人意识到以太坊在这个设计初衷的重要意义。

我们在设计整个SERO-CHAIN时也同样延用了以太坊的这个功能，可以想像，通过链上完成基于共识的交易，首先我们需要降低GAS消耗，以降低链上交易性价比的硬门槛，为此我们设计了新的共识机制，这点在其他章节已经阐述。

假设在共识成本即GAS消耗可以忽略不计的情形下，任何一种Token的价值取决于链上交易的其他成本，这些成本受到数字资产的集中化程度、市场供需关系等影响，这和现实世界的货币并无不同，加密货币同样是用来衡量商品、服务或权益的价值的，因此我们认为开发者发行Token可以有自己的经济模型，这里仅就SERO币的经济模型角度讨论。

站在SERO生态的角度，所有的商品、服务的价值都有一个源头，由于区块链平台本质是一个公平的价值流通市场，因此所有的经济行为的成本底层在于交易成本，SERO币就是交易成本的载体，站在这个角度，SERO币将用于以下激励用途：

- 记账奖励；
- 算力贡献奖励（对于使用了隐私机制的应用，会需要更多的算力消耗）；
- 其它角色包括算法提供者（通过发布智能合约的形式）的运行激励；
- 在SE-Random共识中，SERO的Token持有会影响个别场景下（譬如初始种子节点随机选择）的权重；
- SERO生态的开发者会因其开发应用的实际产生价值而获得SERO的Token奖励，这种奖励往往用于实际补贴其共识记账或算力支付开销的成本方式给出；
- 用户也可以将SERO的Token用于其DApp或SERO相关的生态系统中的各种目的。

第六章 路线图

我们以西方国家家喻户晓的奇幻系列《龙枪编年史》作为版本发布代号。

6.1 秋暮之巨龙（V0.X）

2018.9 AlphaNet 内测网络发布

* 代码开源

* 支持普通交易信息加密

* 支持智能合约

* 支持智能合约发行匿名Token资产

2018.11 BetaNet-RC 公测网络发布

* 发布客户端钱包

* 支持发行匿名Ticket资产

* 去中心化挖矿许可证

2018.12 BetaNet-Release 公测网络发布

* 支持发行Package资产

* 支持暗标和私密场外交易功能的智能合约

* 智能合约代缴手续费

6.2 冬夜之巨龙（V1.X）

2019.3 全球化节点部署，准备主网环境

2019.4 MainNet 网络上线

* BetaNet-Release 上的 SERO Token 映射回 MainNet

* 轻钱包以及轻节点

* 链下计算功能

* SE-Random 共识

6.3 春晓之巨龙（V2.X）

2019.7 隐私三件套另外两件（ALIEN PROTOCOL 和 CASTROL PROTOCOL）上线。

2019.10 增加多方安全计算和链下数据应用隐私保护机制。

第七章 项目生态

7.1 项目团队

Leyla Q.

美籍华人，毕业于波士顿卫斯理女子学院计算机系，美国早期互联网极客，商务社交网站底层架构师、数个黑科技底层协议发明人、GLAB区块链极客组织发起人。

Dr. Leo Xu

美籍华人，毕业于加州理工大学电气工程系、美国密歇根韦恩州立大学（Wayne State University）计算机系终身教授。

Robert B.

古典搜索引擎大数据研发工程师，商务社交网站运营合伙人、美国硅谷SOSV加速器创业导师，数年投融资行业经验。

Jason Pope

曾任中国知名线上地图公司CTO、汽车垂直电商网站技术合伙人、上市公司金融事业部VP兼CTO，GLAB区块链极客组织资深极客。

Durant D.

曾任中国知名旅游上市互联网公司事业部CTO、知名视频网站技术总监、100亿+销售额B2B互联网公司CTO，GLAB区块链极客组织资深极客。

Gordon T.

曾任雅虎资深研发工程师，3721核心研发、知名视频网站P2P协议核心研发、FLASHGET核心研发、100亿+销售额B2B互联网公司首席架构师，GLAB区块链极客组织资深极客。

7.2 顾问

Suyang Zhang

IDG首位荣誉合伙人，中国第一批风险投资人；多年被福布斯评选为“中国最佳风险投资人”及“世界最佳风险投资人”

7.3 生态合作

SERO在早期工作中，获得了MATTER Global和GLAB的技术极客的支持，对此表示感谢。此外，还有一些机构参与了对SERO项目的早期投资，我们会在官网正式披露并正式对这些支持者表示感谢。

第八章 参考目录

[1] MONACO J V. Identifying Bitcoin users by transaction behavior[C]//The SPIE DSS, April 20–25, 2015, Baltimore, USA. Baltimore: SPIE, 2015.

[2] ZHAO C. Graph-based forensic investigation of Bitcoin transactions[D]. Iowa: Iowa State University, 2014.

[3] LIAO K, ZHAO Z, DOUPE A, et al. Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin[C] //The Symposium on Electronic Crime Research, June 1–3, 2016, Toronto, Canada. Piscataway: IEEE Press, 2016: 1–13.

[4] MEIKLEJOHN S, POMAROLE M, JORDAN G, et al. A fistful of bitcoins: characterizing payments among men with no names[C]// The 13th ACM Internet Measurement Conference, October 23–25, 2013, Barcelona, Spain. New York: ACM Press, 2013: 127–140.

[5] ROND, SHAMIR A. Quantitative analysis of the full Bitcoin transaction graph[C]//The 17th International Conference on Financial Cryptography and Data Security, April 1–5, 2013, Okinawa, Japan. Heidelberg: Springer, 2013: 6–24.

[6] GENNARO R, GENTRY C, PARNO B, et al. Quadratic span programs and succinct NIZKs without PCPs [C]//The 32nd Annual International Conference on the Theory & Applications of Cryptographic Techniques, May 26–30, 2013, Athens, Greece. [S.l.:s.n.], 2013: 626–645.

[7] PARNO B, HOWELL J, GENTRY C, et al. Pinocchio: nearly practical verifiable computation[C]//The 2013 IEEE Symposium on Security & Privacy, May 19–22, 2013, San Francisco, USA. Washington, DC: IEEE Computer Society, 2013: 103–112.

[8] REID F, HARRIGAN M. An analysis of anonymity in the Bitcoin system[C]//The 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust, October 9–11, 2011, Boston, USA. Piscataway: IEEE Press, 2011: 1318–1326.

[9] ANDROULAKI E, KARAME GO, ROESCHLIN M, et al. Evaluating user privacy in Bitcoin[C]//The 17th International Conference on Financial Cryptography and Data Security, April 1–5, 2013, Okinawa, Japan. Heidelberg: Springer, 2013: 34–51.

[10] CHAUM D. Untraceable electronic mail, return addresses and digital pseudonyms[J]. Communications of the ACM, 2003: 211–219.

[12] VALENTA L, ROWAN B. Blindcoin: blinded, accountable mixes for Bitcoin[J]. Financial Cryptography and Data Security, 2015: 112–126

[13] SHENTU Q C, YU J P. A blind-mixing scheme for Bitcoin based on an elliptic curve cryptography blind digital signature algorithm[J]. Computer Science, 2015.

[14] RUFFING T, MORENO-SANCHEZ P, KATE A. CoinShuffle: practical decentralized coin mixing for Bitcoin[M]// Computer Security –ESORICS 2014, Heidelberg: Springer, 2014: 345–364.

[15] BISSIAS G, OZISIK A P, LEVINE B N, et al. Sybil-resistant mixing for Bitcoin[C]// The 2015 ACM Workshop on Privacy in the Electronic Society, November 3, 2014, Scottsdale, USA. New York: ACM Press, 2014: 149–158.

[16] DWORK C, NAOR M. Pricing via processing or combatting junk mail[C]// The 12th Annual International Cryptology Conference on Advances in Cryptology, August 16–20, 1992, Santa Barbara, USA. Piscataway: IEEE Press, 1992: 139–147.

[17] CASTRO M, LISKOV B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398–461.

[18] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: anonymity for Bitcoin with accountable mixes [C]//The 19th International Conference on Financial Cryptography and Data Security, January 26–30, 2015, San Juan, Argentina. Barbados: Financial Cryptography, 2014: 486–504.

[19] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from Bitcoin[C]//The 2014 IEEE Symposium on Security and Privacy, May 18–21, 2014, San Jose, USA. Washington, DC: IEEE Computer Society, 2014: 459–474.

[20] VALENTA L, ROWAN B. Blindcoin: blinded, accountable mixes for Bitcoin[J]. Financial Cryptography and Data Security, 2015: 112–126

[21] SHENTU Q C, YU J P. A blind-mixing scheme for Bitcoin based on an elliptic curve cryptography blind digital signature algorithm[J]. Computer Science, 2015.

[22] RUFFING T, MORENO-SANCHEZ P, KATE A. CoinShuffle: practical decentralized coin mixing for Bitcoin[M]// Computer Security –ESORICS 2014, Heidelberg: Springer, 2014: 345-364.

[23] BISSIAS G, OZISIK A P, LEVINE B N, et al. Sybil-resistant mixing for Bitcoin[C]// The 2015 ACM Workshop on Privacy in the Electronic Society, November 3, 2014, Scottsdale, USA. New York: ACM Press, 2014: 149-158.

[24] BEN-SASSON E, CHIESA A, GREEN M, et al. Secure sampling of public parameters for succinct zero knowledge proofs[C]// 2015 IEEE Symposium on Security and Privacy (SP), May 18-21, 2015, San Jose, USA. Piscataway: IEEE Press, 2015: 287-304.

[25] PEREIRAGCCF,JRMAS,NAEHRIGM, et al. A family of implementation- friendly BN elliptic curves[J]. Journal of Systems and Software, 2011, 84(8): 1319-1326.

[26] ARANHA D F, FUENTES-CASTAÑEDA L, KNAPP E, et al. Implementing pairings at the 192-bit security level[C]//The 5th International Conference on Pairing- Based Cryptography, May 16-18, 2012, Cologne, Germany. Heidelberg: Springer- Verlag, 2012: 177-195.

[27] ZIEGELDORF J H, GROSSMANN F, HENZE M, et al. CoinParty: secure multi –party mixing of Bitcoins[C]//The 5th ACM Conference on Data and Application Security and Privacy, March 2-4, 2015.

[28] JENS G. Short pairing-based non-interactive zero-knowledge arguments[C]//The 16th International Conference on the Theory and Application of Cryptology and Information Security, December 5-9, 2010, Singapore. Heidelberg: Springer, 2010: 321-340.

[29] LIPMAA H. Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments[C]//The 9th International Conference on Theory of Cryptography, March 18-21, 2012, Sicily, Italy. Heidelberg: Springer-Verlag, 2012: 169-189.

[30] NIR B, ALESSANDRO C, YUVAL I. Succinct non-interactive arguments via linear interactive proofs[C]// The 10th Theory of Cryptography Conference on Theory of

Cryptography, March 3–6, 2013, Tokyo, Japan. Heidelberg: Springer– Verlag, 2013: 315–333.

[31] BEN–SASSON E, CHIESA A, GENKIN D, et al. Verifying program executions succinctly and in zero knowledge[C]// The 33rd International Cryptology Conference(CRYPTO 2013), August 18–22, 2013, Santa Barbara, USA. Heidelberg: Springer–Verlag, 2013: 90–108.

[32] LIPMAA H. Succinct non–interative zero knowledge arguments from span programs and linear eror–correcting codes[C]//The 19th International Conference on Advances in Cryptology, December 1–5, 2013, Bangalore, India. New York: Springer–Verlag New York, Inc., 2013: 41–60.

[33] BEN–SASSON E, CHIESA A, TROMER E, et al. Succinct non–interactive zero knowledge for a von neumann architecture[C]//The 23rd USENIX Conference on Security Symposium, August 20–22, 2014, San Diego, USA. Berkeley: USENIX Association, 2014: 781–796.

[34] MENEZES A, SARKAR P, SINGH S. Challenges with assessing the impact of nfs advances on the security of pairing–based cryptography[C]// International Conference on Cryptology, December 1–2, 2016, Kuala Lumpur, Malaysia. Heidelberg: Springer–Verlag, 2016: 83–108.

[35] Shunli Ma, Yi Deng, Debiao He, Jiang Zhang, Xiang Xie. An Efficient NIZK Scheme for Privacy–Preserving Transactions over Account–Model Blockchain. Cryptology ePrint Archive, Report 2017/1239, 2017.

第九章 附录

A 法律申明

SERO Token (“SERO Tokens”)的销售内容仅作为针对特定面向的人群或参与者的交换媒介，也不是任何形式的招股说明书或要约文件，也不打算构成任何形式的证券要约、商业信托中的单位、集体投资计划中的单位或任何其他形式的投资，或任何司法管辖区中任何形式的投资的要约。 没有监管机构审查或批准本白皮书中列出的任何信息。 本白皮书尚未在任何管辖区的任何监管机构注册。 通过访问和/或接受拥有本白皮书或其部分(视情况而定)中的任何信息，默认您符合以下条件：

(a) 您不在中华人民共和国境内，也不是中华人民共和国的公民或居民(税收或其他方面)，或居住在中华人民共和国境内；

(b) 您不在美利坚合众国，也不是美利坚合众国的公民、居民(税收或其他方面)或绿卡持有者，或居住在美国；

(c) 根据您所在地区的法律、法规要求或规则，您不在禁止、限制或未经授权以任何形式或方式出售令牌的司法管辖区内，无论是全部还是部分；

(d) 您同意符合以上描述的条件限制和约束。

B 风险提示

本信息并不代表投资建议、或同意销售的许可，以及引导和吸引任何的购买行为。