EID-CHAIN WHITE PAPER

汇金公链白皮书

一种基于区块链技术的身份隐私和数据隐私保护的解决方案

链接未来

CHAIN TO FUTURE

2020.7.8

v1.05

目 录 表

引 言

作为一种新兴的分布式账本技术,区块链存储着用户之间的交易记录和隐私数据,有着开放透明、交易记录无法更改、来源可追踪等特性。物联网、金融、医疗等行业纷纷结合区块链技术来解决行业痛点,所以区块链发展非常迅速,行业规模越来越大。然而,区块链上的数据对全网节点都是公开的,数据的更新操作也是透明的,这会给黑客留下攻击的空间,导致用户信息泄露。

随着区块链技术的发展,用户的隐私无法得到有效的保障,安全问题和隐私泄露问题频频出现,严重影响区块链的应用和推广。区块链本身具备的匿名性和隐私性已经无法满足用户对隐私保护的需求,迫切需要保护数据隐私和用户隐私的新方案。

截至目前，在大部分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的账户信息、交易信息都会暴露。 比特币提供匿名交易，实现发送者和接收者之间一对一交易的关系，并能永远记录全网发生过的交易。但是，比特币只提供低层次的隐私保护，这点在学术界众所周知。比特币交易是半匿名的，在区块链上的每一笔交易都是永久公开的，但每个钱包的主人是未知的，由于每个人都需要把钱包里的币在某个地方兑现，兑现时通常需要把比特币地址与银行账户联系起来，这样一来，把钱包地址与现实世界的身份联系起来就相对容易。所以比特币网络的隐私性没有那么好。

因此，我们可以说，比特币的安全性是受到密码学的保护的，但是隐私性其实并没有。我们可以通过很多方式进行分析，例如根据交易的关联性，交易时间和交易的广播情况等，就可以找到账户对应的个人是谁，从而得知这个人在比特币

上的交易情况等隐私信息。

EID-CHAIN 的目的就是在改善比特币的这一问题。EID-CHAIN 正在尝试使用技术组合的方案实现隐私性。我们在比特币概念以及其他隐私币的基础上进行了一系列的改进，由此诞生出一个去中心化的，且具备更强匿名性的加密数字货币网络，旨在打造一个可无限扩展又安全的隐私价值网络。EID-CHAIN 不仅仅是一个单一的区块链项目，更是一个基于区块链的分布式隐私互联网的多项研究成果的整合，它将在身份安全、网际自由、社交隐私、去中心化金融和商业等多方面发挥重要作用。 为了适应项目的不断进化，让关注本项目的社区用户、开发者和同业研究者对 EID-CHAIN 有持续性的了解，我们将会根据项目进度和研究发展不断升级更新我们的白皮书，力求对项目的 发展现状和未来方向有及时且客观的呈现。

一、 背景

区块链中的隐私保护问题，例如加密货币里的匿名交易、智能合约的隐私、区块链隐私保护基础设施等都是长期的研究热点。按隐私保护技术分类，零知识证明、安全多方计算、同态加密、环签名、代理重加密等，都是依靠密码学技术来实现对数据隐私的保护。而其中，零知识证明作为能实现最强匿名性的隐私保护技术，一直受到各区块链项目的重点研究和探索。从应用的角度来看，区块链技术的各大应用场景，例如加密货币、电子存证、身份识别、金融数据结算等对隐私保护的要求也越来越高。其中，加密货币是目前为止区块链技术最为成功的应用，诞生了诸如门罗币(Monero)、大零币(ZCash)、达世币(Dash)等非常优秀的隐私货币。零知识证明，作为能实现最强匿名性的隐私保护技术，一直受到这

些加密货币项目的重点研究和探索。 零知识证明是由 S.Goldwasser、S.Micali 和 C.Rackoff 在 20 世纪 80 年代初提出的。它是一种证明者能使验证者相信某个论断是正确的，同时这个证明过程不泄露任何有用的信息。零知识证明属于交互式证明系统，除了传统的完备性和可靠性必须满足之外，其特有的零知识性保证了验证者在被证明过程中无法获得证明者拥有的秘密或者任何有助于获得该秘密的其他信息。长期以来，零知识证明作为一种强安全的隐私保护技术，在理论上获得了长足的研究和发展，但是其性能参数包括需要非常多的交互证明轮数、证明的数据长度、生成时间和验证时间，常常是制约该技术获得实际应用的瓶颈。

二、 区块链隐私泄露风险高

其实远在比特币之前，就有一种古老的交易形式可以实现对隐私性非常好的保护：交易双方将钱藏到袖子里达成交易，这样即使其他人目睹了这笔交易，也无法得知交易的金额等隐私信息。但是直接将这样的思路照搬到区块链里并不容易。因为在一个公开的账本里，每一笔交易的合法性需要得到其他人的验证，以确保交易的发起方确实授权了这笔交易，并且这笔交易没有造成恶性通货膨胀。怎么样能既把一笔交易的具体信息“藏到袖子里”，同时又允许其他人验证交易的合法性呢?

我们先来看大家最熟悉的比特币的设计。众所周知，比特币对交易的隐私性保护得并不是很好：在比特币系统里，尽管每个用户都有一个匿名的钱包地址作为在链上的化名/假名，但每个地址所对应的交易记录与信息在上链后其实都是可以通过公开渠道查询到的。通过将与匿名地址有交易往来的用户的信息进行交

叉分析，就可以轻易地追溯到用户的真实身份。

三、 加密交易和范围证明

加密货币交易中的隐私性通常可以分为两类：一是匿名性，即交易双方的身份可以被隐藏起来；二是机密性，即该笔交易的交易金额是不可见的。早期的加密货币项目例如比特币，其交易由于没有把收款人和付款人的比特币地址与他们各自在真实世界中的身份信息进行关联，保证了一定程度的“弱匿名性”。因此如何保证交易金额的机密性就成为了制约比特币和其他加密货币，以及各类区块链项目发展的一大限制。

1. 加密交易

Maxwell 在 2016 年提出了“机密交易”(Confidential Transactions)的概念。注意，比特币等加密货币的交易形式称为未花费的交易输出（Unspent Transaction Outputs，UTXO)，即当前这笔交易的其中一个输入使用的是之前某一笔交易的未使用过的一个输出，并且需要附加当前交易输入地址对应的数字签名。因此，UTXO 模式的交易验证的主要思想是：验证当前交易的每一个输入都是属于 UTXO，并且所有的输入总和大于所有的输出总和。机密交易的思想就是交易金额，即 UTXO 形式交易中的各个输入和输出，用承诺算法隐藏起来；同时，为了支持公开可验证性（否则失去了区块链的透明和可审计的意义)，机密交易还会包含 一段零知识证明，用来证明交易的输入总和大于输出总和，并且所有的输出都是正值。 在机密交易中，交易金额通常用 Pedersen 承诺算法隐藏起来。该承诺算法主要是承诺者先向接收者承诺某个秘密数，即生成某个承诺值，在后面的阶段通过展示该秘密数，由接收者确认前后承诺值是否相等。注

意，承诺算法的两个要求：一是隐藏性(Hiding Property)，即承诺值不能泄露任何关于秘密数的信息；二是绑定性(Binding Property)， 即承诺者给出承诺值后，无法更换承诺中的秘密数，使得在后面的阶段用新的秘密数生成相同的承诺值，从而欺骗接收者。基于椭圆曲线的 Pedersen 承诺算法主要形式如下：Com(v)=v·H+r·G，这里 H 和 G 分别是作为公开参数的生成元，为椭圆曲线上的两个基点，v 是交易数额，r 是一个盲化因子，用来保证语义安全性。Pedersen 承诺方案不但满足承诺方案的两个传统的安全要求，完美的隐藏性（Perfect Hiding Property），和计算绑定性（Computationally Binding Property），而且具备非常好的同态加密性（Homomorphic Encryption），即：
Pedersen 承诺方案的同态加密性，保证了 UTXO 交易中多个输入和多个输出的总和均是 Pedersen 承诺，即交易金额数可隐藏。

2. 范围证明

为了“零知识”地证明机密交易中的输入和大于输出和，需要依赖一种称之为“范围证明”的技术。范围证明主要是证明经过加密或者承诺等隐藏处理之后的某个秘密数，其取值在某一个特定区间内。 大多数的范围证明方案看上去非常适合成为机密交易的一个组成部分，但是它的主要缺点在于需要一个可信任的初始化阶段，以及时间和空间上带来的巨大性能开销。依赖初始化阶段的可信环境，会给该区块链的透明性带来质疑。采用了范围证明的机密交易开始，会变得非常大而且验证缓慢，其中的一个范围证明大小约为几千个字节，且需要几个毫秒才能验证。而传统的 UTXO 交易里的数字签名小于 100 个字节，且验证时间不超过 100 微秒。因此如果能解决这两个问题，那么机密交易看起来就能真正

成为可能。

四、 区块链隐私和安全

1. 区块链隐私和安全

很多时候大家说要在区块链上建立应用，比如医疗，金融，这牵扯到很多隐私性很强的信息。很多人对隐私和安全存在误解，大家讲区块链是很安全的，他们就觉得区块链也可以保护隐私，但其实这两者是完全分开的。区块链的安全是说区块链是一个分布式的系统，那么在每一个节点可能是恶意的，它可能不按照规则来做事情的情况下，区块链的架构可以使得在这种分布式系统，虽然某一个节点是不可信的，但是整个的系统可以保证它一定的规则。所以在这种情况下讲的是它的安全性。但这种安全性跟隐私保护其实是没有关系的。现在的区块链上的大多数数据和智能合约都是公开的，其实没有任何隐私保护。所以大多数区块链可能很重视安全性，但其实是没有任何隐私保护的。

隐私保护是个很复杂的问题，涉及到我们要在很敏感的数据上做计算。比如现在的区块链，没有任何隐私保护，在一个节点做计算的时候，因为数据都是公开的，计算过程中就会被泄露。区块链本身内部存在一些冲突，一方面它是去中心化的，从理论的角度来说确实会有一些低效，所以对区块链应用来说本身有一些劣势；但同时就因为它是去中心化的，跟中心化相比，去中心化的信任模式有很大优势。

2. 余额隐藏机制

区块链是按照时间顺序排列的数据区块链式结构,本质上是通过去中心化的

方式用密码学实现各个环节安全性的防篡改分布式数据库。区块链具有去中心化、防篡改、匿名性、公开可验证、可溯源、代码开源等特点。目前,在绝大多数区块链平台中,任何节点都可以访问区块链上的所有数据,所以区块链隐私安全问题显得尤为突出,成为区块链领域的重要研究课题。当前区块链隐私技术主要围绕基于区块链的可验证计算、区块链数据隐私、区块链交易地址隐私和区块链交易金额隐私等方面展开研究。首先,由于区块链、安全多方计算和可验证同态秘密分享都为了解决不可信群体之间如何协同工作的问题,所以区块链与安全多方计算和可验证同态秘密分享的结合具有先天优势。绝大多数现有的同态秘密分享和安全多方计算存在通信轮数多和通信量大的问题。然而,在区块链环境下,多轮通信和大量的通信数据势必导致算法本身和区块链平台运行效率的降低。除此之外,由于区块链中的节点是不可信的,大量的通信数据将给节点带来繁重的验证负担。因此,研究低轮通信的同态可验证秘密分享与安全多方计算对基于区块链的可验证计算具有重要意义。其次,现有基于区块链的应用中普遍存在泄露数据隐私和难以支持同态计算的问题。因此,研究安全高效且支持同态计算的去中心化外包计算机制可有效解决区块链应用系统中难以支持同态计算和隐私泄露的问题。最后,按照记账方式,区块链可以分为基于 UTXO 的区块链和基于账户的区块链。由于基于账户区块链中矿工需要实时更新动态变化的余额,所以区块链的余额隐藏机制具有一定困难性。因此,目前提供金额隐藏功能的区块链平台都是基于 UTXO 的区块链,而基于账户的区块链平台均以明文方式记录所有交易。所以,研究区块链余额隐藏机制可以弥补现有区块链技术中心缺少余额隐藏机制的不足。

五、 理念和使命

1. EID-CHAIN 的愿景

EID-CHAIN 希望利用分布式的区块链技术重塑价值互联网和隐私的未来。我们不得不承认，中心化的集中模式对于几千年来人类文明的快速发展起到了极大的促进作用，对人类经济社会文化等各方面的发展都起到了巨大的推动作用。但是，随着人类文明的不断进步，社会进入后工业化时代，中心化的运作模式不断限制着人类群体的总生产力提升，直接影响了文明的进一步发展。因此，分布式模式的区块链技术的出现，让我们找到了解决问题的方向，共识体系通过技术手段产生被动信任，形成不可篡改的共识机制，从而达成迄今为止信任的最高境界—无需信任，从根源处解决了现代人类文明发展的瓶颈，值得全人类不断探索和实践。加密货币是价值传递的手段，而区块链为我们带来的不仅是金融的改变，更是一种事物运转的规律发现。它可以为我们带来更多，从金融到商业，从娱乐到文化，从产权到法律，从隐私到自由，从意识到认知。从本质来看，区块链形成的社会浪潮将改写人类文明的历史，再次将整个人类文明带入新一轮高速繁荣发展中。寻找区块链和加密货币的应用价值，一直是 EID-CHAIN 开发团队的目标，也是设计和开发 EID-CHAIN 的初衷，我们希望通过我们的努力可以为世界打开一扇新的未来之门。

2. EID-CHAIN 的使命

EID-CHAIN 通过更加完善的区块链基础设施建设和不断升级，为更多需要使用区块链技术的个人和项目提供更加安全隐私的需求。在客户端提高强度保护

用户隐私，实现标准的非信任制，在客户端直接嵌入相同的匿名层并很好地利用了协议扩展性，让用户使用稳固的系统匿名发送资金时有着更完美的体验。 同时，通过解决传统区块链无法突破的基本性能瓶颈，孵化出新一代去中心化应用 DApp 优质项目。EID-CHAIN 希望能改进其他竞争对手的不足从而改善技术层面的漏洞，提供高技术、高隐私和高拓展性的解决方案，真正带给传统行业可以开发实质性应用的平台。

3. 区块链的扩容问题

区块链的核心价值在于它通过技术手段解决了信任问题，并达成去中心化共识。自 2009 年比特币问世以来，短短十年间，区块链和数字货币已飞速的发展，随着 2019 年各大国际银行、央行和社交巨头 Facebook 先后入场数字货币，数字货币已逐步从小众市场走向了主流社会。不管区块链技术是应用在加密货币领域还是应用在传统实体领域，区块链的性能都是区块链行业不容忽视的“最后一公里”问题，如果区块链的性能没有得到持续的突破，未来，区块链仍然难以承载大规模 C 端市场，当链上同时有千万人交易时，巨大的高并发数只能让区块链更加拥堵，交易更慢。比特币只有 7TPS，以太坊也只有 25TPS，即便是 EOS 宣传的百万 TPS 但实际也只有 700-1300 左右。在经历了 2017 年的市场狂热之后，虚拟货币和整个区块链行业，在市场、监管、认知等各方面都进行了一定程度的调整和变化，数字货币市场正在逐渐回归理性，更多的人开始重视区块链扩容的问题在区块链发展中的重要性。截止到目前为止，区块链的扩容性和速度方面都有着其固有的局限性，使现有的区块链的性能尚无法满足快速的高并发交易。为此，EID-CHAIN 采用安全快速的 Equihash PoW（工作证明

挖掘算法）作为共识算法，突破区块链技术固有的局限，达到了区块链的高度可扩展性、交易极速确认的特性。同时，EID-CHAIN 引入区块链交易信息裁剪技术，采用的最强大的隐私协议 MimbleWimble 协议，利用加密技术来删除大多数过去的交易数据，让 mempool 矿池中已花费 output 与已收入 input 之间进行抵消，从而裁剪掉一些写入区块的不必要的信息。 当前，用户对隐私保护的关注和需求日益增强。过去两年，多家知名公司被先后爆出泄露大量用户隐私数据，包括雅虎、优步、Paypal、洲际酒店、美国信用机构 Equifax、英国国家医疗服务体系（NHS）等等，泄露的数据涉及数千万到数亿规模用户。国际社交巨头 Facebook 也在 2018 年 3 月发生了一次最大规模的隐私数据泄露事件，Facebook 的市值也因此在两天之内蒸发掉数百亿美元，并可能面临高达其 4 倍市值的天价罚款。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因为中心化 平台缺乏足够的数据安全保护机制引起的。因此，隐私区块链系统被认为能从根源上杜绝此类事件的重复发生，然而，比特币和以太坊等区块链网络的设计由于在更早期阶段，而没有充分考虑到去中心化网络与用户真实身份结合的问题，会使区块链上存储的用户数据存在隐私泄漏风险。另一方面，区块链网络中的数字资产及其交易记录，对用户来说是异常敏感的信息，对所有人透明并且不可篡改，这在区块链落地现实场景中后进行大规模 C 端应用时，大部分场景无法实现或者用户无法接受。

4. 匿名支付

在提高隐私和加密数字货币的可互换性时，最大的挑战是，无法做到加密整

个区块链。在以比特币为基础的加密数字货币体系内，能看到哪些输出未发送，哪些已发送，通常将其称为 UTXO，全称是未使用交易输出。这让每个用户在公共帐本中都可充当诚实交易保证者的角色。比特币的协议是在不依赖第三方参与的前提下设计的，即便是在没有第三方的参与前提下，也能通过公共区块链随时读取用户信息以实现审计，这是至关重要的。 EID-CHAIN 的目标是在不失去这些要素的前提下，提高保密性和可互换性，同时我们坚信，这是成功创建数字货币的关键。我们还进行了一系列的改进，例如去中心化、使用链接实现强匿名、相同面值和被动先进的混币技术。我们能让货币本身具备完全可互换的能力。可互换性是金钱的属性，决定货币的各单位都要保持平等。当你以通货的形式接收资金时，资金不应该保留之前用户的使用记录，或者用户能很轻易地撇清之前的使用历史，从而做到所有货币是平等的。与此同时，任何用户在不影响他人隐私的情况下，保证公共账本的每笔交易都是真实的。为了提高可互换性和保持公共区块链的诚实性，我们提议使用先进的非信任制去中心化混币技术，为了保持通货的可互换性，这项服务直接整合到这个货币体系中，对于每个用户而言都可容易和安全使用。

六、 EID-CHAIN 基础系统架构

除了隐私保护的机制之外，EID-CHAIN 的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极其重要，因此，EID-CHAIN 引入了以下技术来增强区块链的底层架构：保密交易协议:采用全球最领先的匿名协议，具有匿名，双签，隐藏发送方、接收方和金额的功能，账本不公开，只有交易双方才能构建自己的账本。 优化共识:使用一种全新的共识机制 Equihash

POW（工作证明挖掘算法)，它结合了最新的理论和加密算法，设计出可以相对兼顾公平和效率的共识机制。交易裁剪:是一种能够实现区块链扩容的方式，众多区块链组合成树形结构，通过对区块中的 交易信息进行裁剪从而实现区块链的横向扩展，不仅满足区块链的兼容性，又有充分的扩展性。

1. 保密交易协议

保密交易（简称 CT）使用了 ECC 椭圆加密算法为基础的承诺方式，称为 Pedersen Commitments。我们先看看 Pedersen 式子是怎么样的?

1）代表 每个 Input/Output 的 C 式子:

C=r*G+v*H

其中，r 即是致盲因子（blinding_factor)，作为私钥使用。r 只有本人知道，是不能被其他人知道的。这个私钥也代表你对这个交易值的所有权；v 则是交易的金额，即 input 或 output。v 仅交易双方知道，矿工与其他人无法知道；G 和 H 是椭圆曲线群的两个发生器点（公钥生成元)。而 r*G 则是 r 在 G 上的公钥，我们没办法透过 r*G 而知道 r 值，这是所谓的离散对数问题（见后文)。我们不会因为知道公钥，就因此而知道私钥。切记不要把这里说的乘法和小学数学中的简单乘法 3*7=21 搞混，概念完全不一样，ECC 在学校里面都未学过。椭圆曲线确保了一件事，交易金额 v 和致盲因子 r 不会被透过逆推的方式而得知，这就是 C 承诺式子，也是 CT 的重要特性。

2）引入了 Excess Value 的式子：

例：

假如 Alice 有 8 元（在 2 个 UTXOs 上，一笔 5 元，一笔 3 元），需要给 Bob 转 6 元，找零 2 元。那么有如下式子：

2 笔输入（Inputs）：

输入 Ci1=r1*G+v5*H，输入 Ci2=r2*G+v3*H

1 笔输出（Change）：

找零 Cchange = r3*G+v2*H

1 笔输出（Output）：

输出 Co=r4*G+v6*H

以上共产生 4 个盲因子：Alice(r1, r2, r3), Bob(r4)

2 笔输入：Alice(v5, v3)

1 笔找零：Alice(v2)

1 笔输出：Bob(v6)

C_alice = (Ci1, Ci2, Cchange)

r_alice = r1 + r2 – r3

那么交易流程即是：

1. **Alice 生成交易数据：**C_alice, r_alice
2. **Alice 发给 Bob:** C_alice, r_alice, v=6, fee=2
3. **Bob 验证：** Ci1+Ci2 = Cchange + r_alice * G + (v + fee) * H
4. **Bob 完成交易数据：Bob 的输出：**Co=r4*G+v6*H

核公钥：K=(r_alice – r4) * G

(Kernel Excess。本次交易公钥)

交易签名：用 (r_alice – r4) 签名

(excess value。本次交易私钥)

矿工验证：

Ci1+Ci2 = Cchange + Co + K + fee * H

用 K 验证签名

3）加了 Offset 的验证式子：

(Ci1+Ci2)-(Cchange+Co+fee*H) = K + offset * G

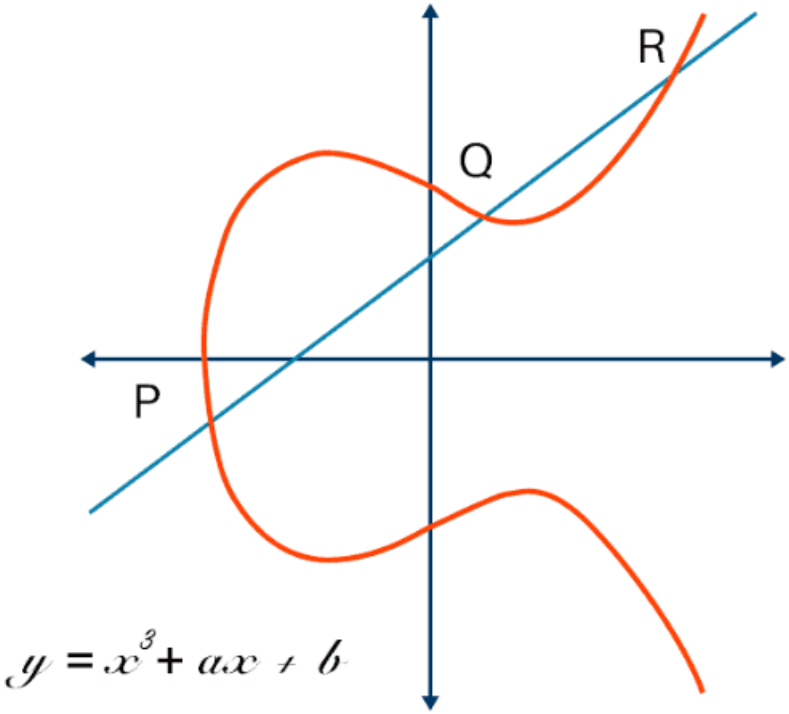
从上面的 C 式子清淅的描述可知，PC 承诺方式是一种使用了离散对数特性的密码学，巧妙将交易金额（v）以及私钥（r） 隐藏了。离散对数的单向性质决定，根据 承诺值 很难计算出对应的明文，但是如果给出明文，则很容易验证它和承诺值是对应的。

ECC 术语或相关重要特性描述如下。

1） **ECC 的离散对数特性**：

密码学建立的基本思想是：某些操作在一个方向上很容易计算，而反向求解却几乎不可能。ECC 的强大之处正是建立在这一反向计算极其困难的离散对数问题，如公私钥算法 DSA，以及 DH 密钥交换算法和 ElGamal 算法等。类似的单向性特征的加密算法还有我们所熟知的因式分解困难的 MD5 算法、以及公私钥 RSA 算法。它们共同表现的特征都是单向性特征明显，MimbleWimble 中的 ECC 尤其如此。

和比特币一样，MimbleWimble 也依赖于椭圆曲线密码学（Elliptic Curve Cryptography, ECC）。在椭圆曲线密码学中，数学运算是在满足特定椭圆曲线的点集范围内定义的。椭圆曲线如下图所示。



这属于数学中的群论，它是抽象代数的一种形式。它使用我们熟悉的数学运算，例如加法和减法。点（也称作“标量”）可以与整数相乘。然而，这些操作是由椭圆曲线在有限域上定义的，而不是我们所熟悉的简单算术，也更不是中学所学过的椭圆。椭圆曲线上的元素可以进行加法和标量乘法的运算，但是除法运算极其困难，这也是这一强大的单向性特征决定，让我们构建了可在非安全通道上的一套强大的加密隐私系统。

在 MimbleWimble 中，公钥由私钥产生。协议选择椭圆曲线上的发生器点，G 或 H 或 J 作为生成元。私钥实际上是一个从非常大的集合（大于等于 2^{128}）中随机选取的整数（标量）。生成元与私钥相乘得出公钥。由于这种乘法极难进行逆运算，使得这些系统得以正常运行。乘法的逆运算（即除法）也称为取对数。因此，这个问题也称为离散对数问题。

2） **同态加密性质**：

所谓的同态加密，即是未加密的数，和加了密的数（Pedersen Commitments）采用同样的运算法则，其结果性质是一样的，这叫同态加密性质。举个例子：明文中的 Alice 身上有 8 元(分别由 2 个 UTXOs 构成：5, 3），需要给 Bob 转 6 元，那么找零 2 元，在 PC 的同态加密性质表现为：

明文：5 + 3 – 6 – 2 = 0

Pedersen Commitments：v5 * H + v4 * H – v6 * H – v2 * H = 0

V5 + V4 – V6 – V2 = 0

无论是直接采用明文，还是私钥*发生器点，或公钥，用同样的计算方法，最终的结果的性质是一样的。零知识证明没有产生多余的钱，交易成功。基于这一加法同态加密性质，我们可确保，在不知道交易金额的情况下，验证等式两边成立。

3） **致盲因子 r**：r 的用途主要用作防止暴力破解 PC 式子 v*H 的 v，以及作为验证私钥使用。它可确保，金额不会在除交易双方之外的第三者中泄露，发送者和接收者不一样的 r，确保交易在隐匿中完成，这是 CT 的实现关键。

4） **excess value（余数）**：因为转账者和接收者使用不同的致盲因子 r，这将导致了结果必然不等于 0，所以才会有这个余数的存在，除了确保等式平衡之外，这个余数也作为整笔交易的私钥，excess_value * G = kernel_excess 即是公钥。任何一笔交易必须满足：sum(outputs) – sum(inputs) = kernel_excess 这个条件。

5） offset（偏移值）： 偏移值的需求是在以上的基础上，进一步增加隐匿性。从而完善整个 CT。它的作用主要为了解决 kernel_excess =输入 Pedersen Commitments 总和– 输出 Pedersen Commitments 总和(包括手续费以及找零)，还是可以通过 kernel_excess 从整个区块的输入输出中找到对应的交易的输入输出，为了消除这种关联性，才在每笔交易增加了一个 offset。使得式子变成：offset * G = kernel_offset, kernel_excess + kernel_offset =输入 Pedersen Commitments 总和 – 输出 Pedersen Commitments 总和。然后在打包区块时，将整个块的所有交易的 kernel_offset 全部加起来成为一个总的 kernel_offsets，这个

总的 kernel_offsets 可以验证区块内交易的合法，又可以隐藏个别交易的 kernel_offset，消除关联性。这是 CoinJoin 要做的事。

具体实现：创建交易时，将 k 分割为 k1+k2，对于交易核(k1+k2) * G，我们在交易核中发布出去的是 k1*G（称之为：the excess），以及 k2（称为：the offset），并跟以前一样使用 k1*G 作为公钥来对交易进行签名。在矿工构建区块的时候，我们对打包的所有交易 k2（the offset）求和，以生成一个单个的聚合值（aggreagte k2 offset）用于该区块所打包的所有交易。一旦区块打包完成并发布和链所接受，其原始的对应每笔交易的 k2 即成为不恢复的。

MimbleWimble 是一个专注于可替代性、可扩展性和隐私性的区块链协议，专门为加密货币设计的隐私协议，依托于强大的加密原语，提供非常好的可扩展性、隐私性和可替代性，它解决了当前几乎所有实现区块链技术（与现实需求之间）差距，协议的性质允许高度匿名的私人交易。即使经过多年的连锁经营，其历史也可以通过简单的计算硬件进行压缩和快速验证。经过多年的测试考验，MimbleWimble 被证明是最具安全性和扩展性的协议，它使用了椭圆线加密技术，简称 ECC（Exploring Elliptic Curve），需要比其他加密类型更小的密钥，在使用它的网络中，区块链上没有地址，网络数据存储非常高效。MimbleWimble 仅需要比特币网络大约 10%的数据存储要求，扩展性更高，存储速度更快，集中度更低。此外，协议的性质允许高度匿名的私人交易（稍后将详细介绍）。 MimbleWimble 协议还具有以下重要特点：

- 在系统上应该可以在双端之间直接传输值并且实现单边交易的模型;
- 所有交易都使用保密交易来避免其直接在链上输出金额;

- 交易应该是非交互式可聚合的，既支持混币技术（CoinJoin），也支持非交互变体，这样可在不了解原始交易的各方，就无法直接的区分它们;
- 对于需要完全节点的新参与者，可大大减少历史区块的同步时间。

2. 共识算法

Equihash 是由 Alex Biryukov 和 Dmitry Khovratovich 设计的工作证明挖掘算法 (POW)。 Equihash 是基于广义的生日问题 (计算机科学和密码学概念) 和增强的 Wagner 算法，它最初由大零币（Zcash）开发，目前，挖掘算法 Equihash 已经被十多种不同的区块链使用，但很多都是由 Equihash 变体演变而来的。Equihash 算法的优点：具有抗 ASIC 性，这种工作证明算法纯粹是面向内存的，意味着挖掘量将取决于硬件的内存量。由于其内存的密集型特性，很难构建经济高效的专用硬件芯片。EID-CHAIN 采用高效安全，适于挖矿的 Equihash POW 共识算法，这一新算法将有助于超 越 ASIC 开发，为未来的 GPU 矿工们提供公平的竞争环境。Equihash POW 算法经过优化，效率更高，可以使用具有更多 RAM 功率的标准 PC 进行挖掘。 EID-CHAIN 实现了 Equihash POW 共识算法，其参数为 n = 150，k = 5，它决定了寻找解决方案需要多少内存空间/带宽。然而，Equihash 允许最初广泛分布的代币和采矿。EID-CHAIN 将设 置参数，为 CPU 和 GPU 矿工提供超越 ASIC 的重要启动。因此，我们将在广泛的民主代币分配 和 ASIC 矿工不可避免但协同的攻击抵抗之间取得平衡。

3. 交易信息裁剪

对区块交易信息进行修剪的目的是为了节省存储空间，在比特币白皮书中，描述了一种回收硬盘空间的方法，即删除区块中除最后一笔交易之外的所有交易。在没有回收硬盘空间里，区块中存储了所有的交易。中本聪在比特币白皮书中明确阐述的是“可将早前的区块大部分数据删除 而只保留区块头数据”来精简目前越来越大的区块数据。这种处理方式既保留了完整的区块信息，又在不影响数据验证能力的情况下精简空间占用。 MimbleWimble 协议仅需要比特币网络大约 10%的数据存储要求，这使得 MimbleWimble 具备高度可扩展性，用于存储区块链，速度更快，集中度更低。MimbleWimble 关于可扩展性的重要特征是“区块裁减（Cut-Through)”。 一般情况下，单个区块包含数百上千笔交易以及其他需要存储在区块链中的大量信息。但是，这些区块可以使用 MimbleWimble 的裁减（Cut-Through）功能进行压缩，从区块中删除大部分信息，而不会有区块链安全性的风险。 下面是一个简单的例子： Alice 向 Bob 发送 1 BTC， Bob 向 Charles 发送 1 BTC。 在这种情况下，典型的区块有两个 UTXO，第一个 UTXO 将保存该 1BTC 的输入，反映它如 何到达 Alice，第一个 UTXO 的输出是事务的结果，它验证比特币现在归 Bob 所有。第二个 UTXO 包括第一个 UTXO 的输出，现在是第二个 UTXO 的输出，以及第二个事务的输出到 Charles。 这意味着 MimbleWimble 裁剪了第一个事务的输出和第二个事务的输入，输入与输出相互抵掉，不用将转移过程写入区块。整个过程就只有一个输入和一个输出，它验证了 Alice 如何获 得这个比特币以及 Charles 如何获得他们的 1 BTC，而不是每个过程都有两个输出和输入。 这会压缩区块链的大小，使 MimbleWimble 在数据存储方面更轻松，可以将区块

扩容达到每秒大量的状态更新，Cut-Through 带来的无限延展性，从而在区块链上支持全球范围内的大量去中心化金融应用，并依赖底层的区块链来强制交易状态提供交易隐私保护。交易信息裁剪有很多优点：

- 交易双方可以选择带隐私保护的交易；
- 能为数字资产转移、交易提供隐私性保护；
- 为数字资产持有者提供匿名性保护；
- 具有场景的延展性；
- 能够成为多种数字货币兑换的分布式平台；
- 以数字货币为媒介完成数字资产的交易。

比特币目前有接近 4 亿笔的交易，但是 UTXO 里大约只有 6000 多万个 Output。新用户若想加入比特币网络，就得先知道過去所有的 400+GB 挖矿历史，才能验证最新的块。而如果应用 Mimblewimble 的方式，区块链的交易历史会被舍弃，只留下大约 100GB 的历史交易 kernel，這樣处理数据时的复杂度即会减少很多。当然，Mimblewimble 的 UTXO 需要附带每个输出的范围证明，这是一个额外的负担，但是这个负担仅与 UTXO 的大小有关，而与整个链已经运行的时间无关。此外，采用了新的技术后，范围证明的尺寸和验证效率都有了很大的改进。

七、 EID-CHAIN 优势和技术突破

1. 支持发行自定义隐私 token

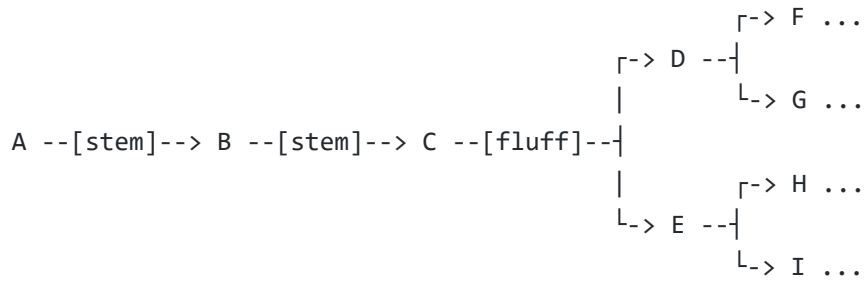
区块链的 token 是从以太坊订立的 ERC20 标准中被广泛认知，在 ERC 标准上，每个人都可以发行自定义的 token，这个自定的 token 可以代表任何

权利和价值，取决于设计 token 时如何赋予。然而目前支持发行 token 的公链绝大部分不支持原生隐私交易，需要由 token 合约撰写者编辑隐私算法，并且需要为他的 token 开发专用钱包，如此发行一个隐私 token 的整体成本就比较高。 在 EID-CHAIN 上，发行方可以很容易地通过 PC 端钱包，并且根据自己项目的需求设定 token 发行总量，就可以在几分钟之内发行一个属于自己的隐私 token。并且，用户自定义发行的 token 继承了 EID-CHAIN 的所有隐私特性。另外，EID-CHAIN 钱包可以直接显示用户的所有隐 私资产而无需单独开发一个专用钱包，从而大大降低项目成本。此外，其它公链上的 token 项目方也可将自己的 token 一部分转移到 EID-CHAIN 上面发行等值的隐私资产，以满足部分现有用户对隐私交易的需求。

2. 交易广播采用升级版的蒲公英协议

蒲公英协议主要目的同样是为了改善比特币交易的隐私性，要知道比特币交易传播并不能很好地隐藏交易的来源，每当进行一笔交易时，它就会向全网的节点公开，因此人们可以追根溯源至初始节点。而蒲公英是一种新的交易广播机制，其目标是混淆比特币交易的 IP 地址。 与蒲公英的花瓣所包含的茎干（Stem）和绒毛（fluff）一样，蒲公英协议分为两个阶段广播到网络：“茎干”阶段（交易被混淆）；“绒毛”阶段（广播出去）。“茎干”阶段每个节点将 交易传达到单个随机选择的对等节点。以某个固定的概率为准，交易会转入为“绒毛”模式，之后再使用普通的广播进行传达，此时将其映射回原始节点变得极具挑战性，因为初始阶段的随机节点被混淆了，这可以防止监视节点使用蒲公英将交易映射回原始地址。EID-CHAIN 的交易广播采用了升级版的蒲公英协议，在原有的基础

上，交易图的保护隐匿更进一步，从而更有效地的保护了发送方的原始 IP。



3. 采用 EquiHash PoW 算法

ASIC 的出现使得算力空前集中在少数矿池/矿工手里，从而降低了网络去中心化的程度。目前抗 ASIC 的方式，一般是给 ASIC 增加内存压力或传输压力，Equihash 便是一个内存（RAM） 依赖型算法，它由 Alex Biryukov 和 Dmitry Khovratovich 联合发明，其理论依据是一个著名的 计算法科学及密码学问题——广义生日悖论问题。 EID-CHAIN 在上线初期采用 EquiHash PoW 算法抵抗 ASIC 矿机，能够有效解决算力集中化问题，同时，Equihash 算法使得挖矿门槛更低以及更加分散化。 我们同时在探索增加其它算法，以让其它非 ASIC 设备可以加入矿工队伍，从而实现更大的去中心化效果。

4. EID-CHAIN 支持审计

任何情况下，企业/团体/个人使用 EID-CHAIN 进行交易都能很好的保护财务隐私，然而在某些场景下，他们需要接受财务合规审计。EID-CHAIN 支持审计，只要资产拥有者提供公钥给审计人员，审计人员就可以获得资产拥有者的资产信息，但审计人员仅能查看而无法使用这些资产，审计功能需要开发专用钱包。

八、 应用场景

隐私保护是现实世界中个人与组织都强烈需求的，尤其在数字世界。EID-CHAIN支持隐私交易，提供各类相关隐私组件，支持不同通证经济生态的拓展。由 EID-CHAIN 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 EID-CHAIN 发行自己的匿名资产，建立自己的隐私生态，这极大提升了区块链的隐私保护机制和水平。

1. 财务合法隐私

财务隐私合法使用案例的范围很广，世界上发生的大多数交易都需要财务隐私，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。在现实世界中，我们遇到的与财务隐私相关的棘手问题可能是这样的：一家公司想要保护一个不让竞争对手知道的供应链信息，一个人不想被公众知道她正在向破产律师或离婚律师支付的咨询费用，一个富有的人不希望让潜在的犯罪分子了解他的行踪，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。同时，对于那些投资银行、对冲基金和其他（证券、债券、衍生工具）交易类型的金融实体，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，从而影响的他们盈利能力。 然而在智能合约中，完整的财务行为序列都会通过网络传播并记录在区块链上，所以是公开透明的，由于他们的金融交易（例如保险合同或股票交易）是高度机密的，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，现在却由于区块链的公开透明性而无法做到。 所以，这对那些不想被

人知道自己财务状况的个人和企业来说，缺乏隐私保护反而是区块链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去中心化应用普及落地的瓶颈，故而相关领域的技术发展进程也备受公众关注。

2. 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会让企业泄露商业机密，这对以往的区块链来说是极大的难题，而在 EID-CHAIN，则可以完全解决商业机密暴露的难题，同时，让参与各方能够享受到应用EID-CHAIN 区块链系统带来的效益提升。

3. 游戏交易隐私

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，同时还要兼顾交易的隐私保 护。目前 EID-CHAIN 是唯一能做兼顾以上功能及交易隐私的技术方案。

4. 去中心化金融

去中心化金融建立区块链技术与网络的普及提供给大众另一个选项：替代原本只有中心化金融机构能提供的服务，让原本无法享受到类似服务的人能够以更便利的方式使用类似的服务，或是以更廉价的方式提供给原本的使用者。 但同样的，在未来去中心化金融将会陆续接受政府和监管机构的监控和管理。许多同类型公司并不希望客户资讯或是金钱纪录在公链上透明化，容易被有心人士利用，进行不法或不道德的行为。而 EID-CHAIN 将会提供更多公司在去中心金融

商业用途上的隐私应用和安全。

5. 合法化区块链应用程序

未来区块链应用程序或将实行实名制，届时会有更多的商业应用希望能够保护用户的信息与数据，同时用户也不希望暴露个人信息。这时隐私链所具备的密码学、时间戳、数字签名等技术特性将赋予用户对数据拥有真正的控制权。 除了以上几种应用之外，EID-CHAIN 还可以应用到更加广阔的领域，只要有更多的涉及到资产数字化，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，都能应用 EID-CHAIN 区块链系统。

九、 发展历程与整体规划

EID-CHAIN 公链的整体发展和实施路线分四个阶段，分别为：

（1）第一阶段，筹建团队

团队建设，技术、运营团队搭建，对接各地政府落实各地由政府牵头筹建区块链产业园，成立基金会。

（2）第二阶段，主网上线

主网测试上线，矿池节点开发/交易所 API 接口开发/DEFI 质押开发

（3）第三阶段，DBP 新引擎开发

单边交易/混合共识 DBP 新引擎/智能合约开发

（4）第四阶段，DApp 应用开发

DApp 应用开发/跨链异构框架设计/分片开发

第一阶段筹建团队，已完成

经历两年的精心打造，EID-CHAIN 公链团队组建技术结构搭建已基本完成，已对接完成武汉、深圳、东莞、厦门、杭州等地政府快速落地区块链产业园建设。基金会已初步设立完成，会议组织各项章程及财务政策正在积极出台中。

第二阶段主网上线，已完成

第三阶段 DBP 新引擎，全面开发中

第四阶段 Dapp 应用开发，技术组方案整理中

技术开发成果：软件著作权 11 项

（2）基于数字资产结算和交易系统

（3）基于数字资产结算独立算法系统

（4）基于区块链数字社区服务管理系统

（5）基于 5G 设备存储和电子存证系统

（6）基于资产数字化区块链管理评估系统

（7）基于区块链数字资产硬件存储管理系统

（8）基于区块链数字智慧城市政务管理系统

（9）基于公链去中心化技术应用开发系统系统

（10）基于资产锚定数字化通证消费确权登记系统

（11）基于公链多节点签名联盟方案资产锚定跨链系统

（12）基于固定资产和无形资产对标区块链数字化通证发行和存储系统

十、 免责声明

请您仔细阅读本免责声明。您也可通过咨询法律和财务专家获取进一步指导。本白皮书包含的信息可能不完整，您同意我们的阐述并不意味着构成了合约关系，尽管我们会尽一切努力确保本白皮书中所阐述的信息是最准确和最新的，但这些材料绝不构成专业建议。EID-CHAIN Foundation 其关系企业既不保证也不对此内容的准确性、可靠性及完整性承担责任，白皮书的内容可能随时更改，有意投资该平台的个人，应在采取本文所载任何信息之前寻求独立的专业建议。

非证券 EID-COIN 的使用与购买带有巨大的财务风险。EID-CHAIN Foundation 及其关系企业在此公开声明，于其平台上所发生的任何交易皆不以任何方式涉及任何司法管辖区对于证券授予的规定，本平台上所发布的所有文件也未教唆投资。 EID-COIN 免责条款，EID-COIN 的使用与购买带有巨大的财务风险。EID-CHAIN Foundation 及其关系企业并未提供投资、财务或法务建议，我们所提供给您的文件，并不能视作专业建议或作为独立事实验证。在进行任何投资决策或采取任何行动（包括但不限于任何 EID-COIN 的购买）前，您必须保证您已对此进行过研究与分析、自行验证过您所想要依赖的任何资讯、考量过您个人自身的投资状况与目标，并且已从适当的专业人士处获得独立的财务建议。您也知悉并同意 EID-CHAIN Foundation 及其关系企业对您并没有任何尽职调查或诚信忠实义务等责任。 平台安全性现在，您已知悉通过 EID-CHAIN Foundation 及其关系企业所存储或传输的资讯可能因各种原因导致无法取回的损失、损毁或暂时无法使用等后果，这类原因包括软件故障、第三方供应商的协定变更、网络中断、不可抗力事件或其他灾害，也包含第三方分散式阻断服务

（DDoS）攻击、已排程或未排程的维护，或其他可控或不可控因素。因此，您必须自行对通过 EID-CHAIN Foundation 及其关系企业服务存储或传输的所有资讯负责，并且必须自行备份及维护其复制副本。 无责任条款 EID-CHAIN Foundation 及其关系企业和与其相关的任何人或法律实体，包括但不限于其代理人、雇员、员工、保险人、律师、继受人及受让人，皆不对您因使用EID-COIN所承受的任何损害、花费或其他损失负任何责任，包含合约、侵权（包括过失）或其他责任。低流动性与价格波动性市场上可能沒有对 EID-COIN 的需求。

EID-CHAIN Foundation 及其关系企业对于 EID-COIN 在市场上的流通及交易声明不负任何责任。Token 在市场上进行交易时，价格波动性通常极高。价格在短时间内剧烈震荡的情形经常发生；此处所谓“价格”， 可能是以比特币、以太币、美元或其他加密货币或法定货币计价。这些波动可能源自于市场动能(包含投机活动)、法规变动、技术创新、其他交易方式的可行性及其他客观因素，并且反映对 Token 供需平衡的变化。因此，EID-CHAIN Foundation 及其关系企业对于 EID-COIN 的可用性或价值，不做任何明示或默示的声明或保证。您理解并接受对于您所持有的 EID-COIN 可能带來的任何利益，不存在任何保证或担保。使用者的法律遵循您了解并同意 EID-CHAIN Foundation 及其关系企业对于决定哪些法律、规则或规范会适用或可能适用于交易不负责任 （包含但不限于任何反洗钱相关法令、证券交易法及税务法规)。 您了解并同意对于可能适用于您的交易所有相关法令自负遵循的义务。在不影响前述条款的情况 下，您了解并同意您对购买 EID-COIN 所产生的税务义务承担全部责任。同时，您了解并同 意 EID-CHAIN Foundation 及其关系企业不直接或间接承担服务所产生的任何税务义务。