零熵白皮书

- 解决了存在于以太坊等当前区块链技术中智能合约的安全问题
- 多元价值体系和可拆分通证技术使其有着最广泛的应用
- 唯一真正的土地链
- 高效和可扩展的共识算法

howard@discoverlaws.com

徐皓

版本 V1.3 2023/3/15

保 密 义 务 告 知

这份文件包含零熵商业机密信息，仅限于供投资者考察投资零熵项目之用。接收本文件表示您同意：

1. 不复制、散发、传播、透露、或公开本文件的内容；

2. 不将从本文件中获得的信息用于其它商业、研究、或投资项目。

目 录

一、 项目概述

在本白皮书中我们将介绍一个新一代区块链公链项目。该项目的核心是一组解决当前区块链行业中一些最迫切问题的技术。这些问题包括:

A. 智能合约的安全性问题。仅 2020 一年，由于智能合约的智能合约的安全性问题就导致用户损失 900 亿元人民币。

B. 应用范围狭窄的问题。与所描述的前景相反，在金融领域之外，区块链技术的应用比较少。一个主要原因是区块链难以表达这些领域所需要的复杂价值形态。

C. 低效问题。最快的公链也只是每秒处理几百笔交易。

为了解决这些问题，我们开发了一个新的公链，称为零熵。零熵有:

- 安全的智能合约模式，彻底消除了通过智能合约盗取用户资产的问题。
- 通用可拆分通证使区块链技术能够应用于前所未及的广泛领域。
- 双链架构消除了任何理论上性能提升的极限。处理交易的能力与节点的计算能力同步增长。

零熵主网已经于 2020 年 7 月上线，至今已经产生了 1600 多万区块（比特币至今只产生约 80 万区块)。这里我们将对零熵技术作一介绍。

二、 背景介绍

区块链是当前信息科技领域最具革命性的新兴技术之一。它通过网络中多个节点共同记账的方式，把数据（区块）按照时间顺序进行串联（链），形成时间

顺序上可追溯，且不可篡改的交易记录。区块链的核心价值在于实现不可篡改、安全可靠的分布式记账系统。基于密码学、分布式共识协议、点对点网络通信和智能合约等技术保障，使用区块链账本系统的多个参与者，无需额外的第三方担保机构，即可构成多方交易的信任基础。进而实现可信的低成本、低延迟信息交换和交易处理，实现数字价值的高效流通。虽然经过 10 多年的发展，区块链技术取得了相当的成功，但目前依然存在一些亟待解决的根本性问题，包括：

A. 智能合约的安全性问题

2013 至 2014 年间，Vitalik Buterin 发表了以太坊白皮书提出用区块链储存程序，用户可以在节点上调用这些程序，通过这种方式，程序可以作为创建者的代理人自动执行交易而无需人的参与。这就是智能合约。Buterin 认为这种机制足以安全地进行程序化的交易。这是一个百亿级的错误。仅 2020 一年，由于智能合约安全性的问题就导致价值 900 亿元加密资产的蒸发。

在以太坊及大批模仿者中，每个智能合约都管理自己发行的代币的账本。也就是说，在这些区块链上存在不止一个账本。原生币有一个账本。每一种代币又各有一个账本。他们都是去中心分布式账本吗？对于原生币的账本不存在争议，对于代币的账本，我们需要考察一下什么才是一个去中心。

所谓去中心指的是每个记账者（矿工）独立地决定各自所纪录的账本内容，而不是机械地复制他人的账本。这种独立性包括独立地决定每一笔交易是否合法，从而是否纪录该笔交易。只要网络中造假者不占优势，就可以通过这种方式阻止非法交易成为区块链网络的共识，从而达到保护资产安全的目的。如果一个区块链中的矿工不具有这种独立决定每一笔交易是否合法的能力，那么这个区块

链就不是去中心的，矿工们都必须依赖一个中心化的权威决定来决定每笔交易是否合法，因此所有账本就是由一个中心来控制的，这个中心就可以任意决定资产的归属，区块链就不能为用户提供安全性保障。而根据以太坊的智能合约交易模式，智能合约代币的账本是由合约管理，而非矿工管理。而每个合约都是由单一的项目方发布，矿工虽然纪录合约所产生的数据，但矿工并不理解这些数据，只能是合约要求矿工记什么矿工就记什么。这就是把所有矿工从记账人变为记账的笔，而指挥这些笔的人是合约的项目方。因此这些代币的账本不是去中心的，而是中心化的账本。这是非常不安全的。

以太坊的智能合约甚至都不能称为合约。没错，合约可以通过程序执行，但并不是每个程序的执行都是一个合约。一个程序的执行要构成合约还需要额外满足一些条件。对于作为去中心化账本的区块链来说，很重要的一条就是交易必须经过验证。正如中本聪所说的：不要信任，要验证。这是区块链的金科玉律，任何时候违反它必然导致安全性问题。但以太坊并不验证智能合约的交易结果，而只是验证智能合约的执行过程。在以太坊中，用户调用智能合约时，节点会执行智能合约，只要智能合约成功返回，节点就认为交易合法并予以记录。这种模式有什么问题呢？毕竟智能合约调用是用户发起的，难道不应该接受智能合约调用的结果吗？这是以太坊的思维。

法律上，双方意思一致才是合约。合约各方必需对各方的付出和获得都达成一致，合约才能成立。那么用户在调用智能合约时，他同意的是什么？是接受智能合约所产生的任何结果，还是合约发布者宣称会产生的结果？绝大多数用户都不是程序员，不可能知道程序会怎么运行，显然他们同意的是合约发布者宣称会产生的结果。但是以太坊是不可能验证智能合约的执行结果是否与用户的预期

（也就是合约发布者宣称的结果）一致，因为以太坊节点根本就没有这方面的信息。所以以太坊中所记录的每一笔智能合约交易只是证明“智能合约产生了这样的结果”，而不是“合约双方同意这样的结果”。混同这二者的后果是致命的。

更糟糕的是，以太坊将智能合约的交易结果作为合约的数据来储存。即，用户从智能合约那里获得的资产是记录在智能合约自己的账本中，而不是公共账本中。以太坊节点本身不会验证这些资产的转移。这些资产的转移是由智能合约处理和验证的。用户不能直接控制这些资产。是智能合约在控制它们。这简直就是开门辑盗。所以结果就是以太坊用户只能任凭智能合约处置，在智能合约面前没有任何安全保障。既没有交易安全，因为以太坊不能保证合约执行的结果符合用户期望；也没有价值储存安全，因为智能合约可以不经用户同意就转走用户资产。

因此我们看到以太坊自发布以来已经发生多起与智能合约有关的安全性事件。相比之下，比特币从未发生过安全性事件。大家都认为智能合约的安全问题是开发者的错误和疏忽所导致，所以业内在规范智能合约开发流程，对于智能合约进行形式验证，代码安全性审计，开发安全的智能合约语言等方面作出了很大的努力。然而智能合约的安全问题从根本上说是自以太坊发布以来业界对于去中心合约的错误理解和由此而来的不当交易模式所导致。解决了这个问题就能杜绝迄今为止的大多数智能合约安全问题。而不解决这些问题，现今的各种努力终归不能杜绝智能合约的安全隐患。

B. 价值表达

绝大多数区块链中，价值是用单一数值来表示的。近来业内提出了 NFT（不

可混合通证）用于代表如艺术品这种独一无二的物品。这是目前区块链所能处理的二种价值形态：或者是不可分的通证，或者是只能算术拆分的通证。

现实世界的资产需要丰富得多的价值表达方式。例如土地不能用单一数值来表示。要描述一块土地必须描述其位置、形状、大小。但另一方面，土地是可混合的。土地可以合并和拆分。此外土地有权益，土地按权益可以分为所有权、抵押权，租赁权等。事实上现实中的一切资产都是有权益的，是权益给了资产价值。没有权益的资产没有任何价值。因此在价值表达方面，当前的区块链技术远远不能满足实际需要。其结果就是区块链技术目前主要只用于金融等少数领域。大部分世界尚未从这一技术中获益。

C． 性 能

区块链一直存在性能问题。比特币网络每秒只能处理 7 笔交易，以太坊 25 笔。普遍认为区块链技术中存在一个不可能三角：即在分散性，安全性，效率三者之间，不可能同时提升这三者。目前所有区块链性能上的提升都是以牺牲分散性或安全性为代价的。

三、 零熵技术概要

零熵从多个方面创新了区块链技术，解决了上述区块链问题。零熵的创新包括：

1. 明示合意智能合约：零熵在比特币式的 UTXO 交易模型中增加了智能合约调用，并允许交易参与各方（自然人和智能合约）通过 UTXO 交易模

型表达各自的意愿。智能合约执行完成并不自动代表交易合法，节点会验证各方的意愿是否满足，如果任何一方的意愿没有满足，则交易不成功。交易的结果以 UTXO 输出的方式交付各方。因此各种智能合约安全问题得以避免。

2. 通用通证：零熵首创一种功能强大的通用的价值表达方法，无论是单纯数值型的，不可混合型的，还是可混合非数值型的价值都可以在零熵上予以表达。在零熵上各种形态的价值都具有平等的地位，通过 UTXO 形式的交易进行交换。
3. 通证拆分：零熵以通证表示价值。通证可以包含权益，用户可以按任意标准对权益进行分割，并按所确定的标准拆分或合并通证。
4. 土地通证：零熵中价值可以不是一个数字。零熵中有一种特殊的价值形态：多边形。土地作为一种重要的资产无法以单一数值表示，但多边形可以。零熵的土地通证是以多边形为价值形态的通证。在零熵创世区块中有代表整个地球的土地通证，所有其它土地通证均由该通证拆分而来，因此保证了每个土地通证唯一地代表了一块土地，在涉地应用中有广泛的使用价值。
5. 高效共识机制：零熵采用新的共识算法，在不牺牲安全性和分散性的情况下，达到了 2000TPS 以上的交易速度和 3 秒的最终确认速度。这种算法没有理论上的性能上限，交易处理能力随节点算力增长。
6. 行签名扩展：在比特币的签名有单行模式。即只对交易中同一位置的输入和输出进行签名。零熵对其进行了扩展，可以用户灵活地协同构建交易。

四、 零熵实现方案

1、通证

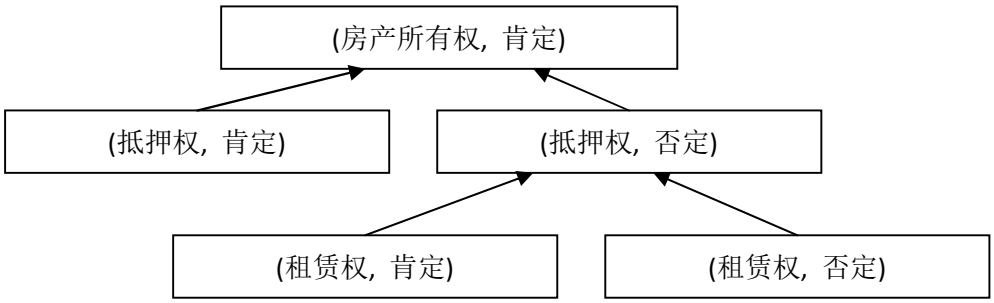
通证代表价值。区块链的应用范围很大承担上受限于其表达价值的能力。在零熵上，通证是一个三元组：类型（一个 64 位数值），价格（一个 64 位数值或哈希值），权益集（代表一个集合的一个哈希值）。这为各种价值形态提供了一种统一的表达方式，并允许根据权益对通证进行拆分。

所有通证在交易中都有平等的地位。即节点接收含各种通证的交易，对它们记账，并按其类型进行合法性验证。而在以太坊中，以太币具有特殊的地位，节点只对以太币记账，验证以太币的交易；而对于智能合约发行的各种币，则由智能合约记账和验证。以太坊的很多安全性问题都来源于这种由智能合约而不是由节点记账和验证的方式。

2、权益和通证拆分

应用可以定义附属于通证的权益。零熵用一种树型结构表达权益之间的关系。权益是一个三元组，包含：父权益的哈希值，权益内容（用户选择的任意文字），肯定/否定的标识。权益之间可以存在父子关系。二个权益如果它们其它内容相同，唯有肯定/否定的标识相反，则称为兄弟权益。在权益集中，任何一项权益可以用其一对兄弟子权益替换，反之亦然。一个通证可以拆分为其它内容相同，但权益集分别为原权益集的二个互补子集的通证，反之亦然。权益集可以描述现实中任何权利的组合。例如：一个含有“土地所有权”权益的通证可拆分为

其它部分都相同，分别含有“土地承包权”和“非土地承包权”权益的二个通证。通过这种方式，用户可以根据需要拆分通证。例如：



业主拥有带(房产所有权，肯定)权益的房产通证。当向银行贷款时，业主可以将(房产所有权，肯定)权益拆分为(抵押权，肯定)和(抵押权，否定)，并生成相应的二个通证。业主将带(抵押权，肯定)的通证给银行，自己保留另一个。当他出租房屋时，可以将(抵押权，否定) 权益拆分为(租赁权，肯定)和(租赁权，否定)，并生成相应的二个通证。业主将带(租赁权，肯定)的通证给房客，自己保留另一个。贷款还清、租赁到期后，业主收回相应的通证，进行合并又成为带(房产所有权，肯定)权益的房产通证。如果中间业主要卖房，业主拿不出带(房产所有权，肯定)权益的房产通证，买家就知道房屋权益不完整，就不会买房。这个例子说明零熵无需知道“抵押权”、“ 租赁权”这些词的涵义也能为房产提供一种安全的交易机制。这种机制的应用当然不限于房产交易。可以说任何现实中的交易都涉及权利的转移，因而可以利用前述机制。

3、交易

零熵使用扩展 UTXO 交易模式。扩展 UTXO 交易中包含输入、定义、输出三个部分。其中输入部分的每个输入项与比特币交易的输入项类似包含对之前交

易未使用输出的引用和签名。定义中的每个定义项或者定义一个几何体(边界线，多边形)，或者定义一个权益项（权益三元组）或权益集（权益项哈希值的集合)。输出中的每个输出项包含一个通证和一个脚本。脚本可以是比特币中那种锁定脚本，也可以是智能合约调用脚本。

4、智能合约

4.1、目前区块链智能合约中的问题

目前区块链中智能合约所采用的都是以太坊式的智能合约。其特点是，用户发起智能合约调用后，只要智能合约执行成功，无论结果是否符合用户预期，节点都认为交易合法并记录进区块中;交易的结果作为智能合约的数据存放在区块链中，特别是智能合约用户的账本也由智能合约保管，导致用户不能脱离智能合约而独立地证明其资产所有权。这种模式不是法律意义上的合约，更导致了一系列安全问题。

法律上，双方意思一致才是合约。但目前的智能合约模式不允许验证双方意思是否一致。虽然可以说用户在调用智能合约时通过参数表达了他的意思。但这种意思只有智能合约可以理解，节点是无法理解。而智能合约对参数的理解是否与调用者的理解一致，节点是无从验证的。因而只要智能合约执行成功，节点就只能认为交易合法。所以目前的智能合约模式是以智能合约对参数的理解为准的，即将智能合约单方面的意思当作是合约的内容。假如用户通过智能合约购买某种产品,用户以为某个参数的单位是公斤,而智能合约认为该参数的单位是斤，则最终用户只能得到他所预期一半的产品。

但这种误解导致双方意思不一致还不是目前智能合约中最严重的安全问题。最严重的是由智能合约保管用户资产。以太坊白皮书中称智能合约是合约发布方的代理人，但目前的智能合约模式中却由智能合约对用户自合约取得的资产进行记账，这就违背了智能合约是发布方代理人的定位，而是采取了代理人和中立记账人的双重定位，是既当球员又当裁判员。近来多起 DEFI 跑路事件的根源就在于这种双重定位允许智能合约发布方盗取用户的资产。即使智能合约发布方是诚实的，黑客也可以通过合约程序的漏洞盗取用户资产。而程序总是会有漏洞的。

这种智能合约模式违背了区块链去信任的本质。任何智能合约都只有一个发布者，区块链能保证的仅仅是在每个节点上所发布的智能合约代码是一致的，并不能验证代码的安全性。如果智能合约严格地只是发布者的代理人，这不会导致安全性问题。但当智能合约也扮演记账者的角色时，其所记的账就是一种中心化的分布式账本，与区块链的去中心化分布式账本有本质的不同。所以用户必须信任智能合约（也就是信任合约发布者）才能放心地交易，为此出现了智能合约审计公司。事情至此已经变得可笑了：作为去中心化、去信任的区块链竟然要依赖中心化的代码审计公司来提供信任。在 DEFI 跑路事件中，我们看到大多数跑路的智能合约都是经过审计的，这充分证明了这种智能合约模式的失败。

4.2、明示合意智能合约

零熵提出了明示合意智能合约模式。在这种模式中，用户可以表达对交易结果的期望，智能合约则试图满足用户的期望，也可提出自己的期望，节点验证双方的期望都得到满足后才认定交易合法。这种模式包括：

- 用户提交 UTXO 式的部分交易
- 节点启动虚拟机执行智能合约调用
- 智能合约向交易中添加输入、输出、或定义
- 节点验证交易完整性，完整的交易才打包进区块

我们以一个例子来说明这种模式。假设某个智能合约发行一种α币，并宣布用户可以用 2 个ω币换 5 个α币。希望进行交易的用户则可以向节点提交一个不完整的交易如下：

输入	输出
UTXO（2ω）	2ω + 合约调用脚本
	5α + 用户锁定脚本

该交易表达的意思是：用户拿出 2 个ω币给智能合约，要求得到 5 个α币。由于该交易的输出中有智能合约调用脚本，节点执行智能合约程序，执行中智能合约向当前交易的输入列表中添加属于该智能合约的 5 个α币 UTXO，并返回成功。

输入	输出
UTXO（2ω）	2ω + 合约调用脚本
UTXO（5α）	5α + 用户锁定脚本

节点验证交易的完整性，即各种币的输入和输出是否相等。由于智能合约所添加的输入与用户所要求的输出相等，该交易合法。如果智能合约添加的不是含 5 个α币的 UTXO，而是 4 个或 6 个，则交易会被判定为不合法，双方都不会有损失。

由于用户得到了一个 UTXO 输出，所以无需依赖智能合约为其记账，即使智能合约仍然维持一个账本，这个账本也没有外部效力，不影响用户资产的所有权。

因此无论是智能合约发布者还是黑客都不可能盗走用户的资产。

当然由于智能合约漏洞，黑客可能盗走属于智能合约的资产。这种安全性问题在性质上与用户未保护好自己的私钥导致资产被盗无异。智能合约的发布者只能责怪自己。

明示合意智能合约中合约不是单纯地满足用户要求，合约也可以表达自己的要求。例如在货到付款的场景中，用户发起交货的合约调用，合约执行时就可以通过向交易中添加以合约为付款对象的输出来提出付款的要求,用户如果没有提供相应的输入，则交货不成功。

明示合意智能合约由于采用 UTXO 模式,因此允许在一个交易中有多个智能合约调用，从而实现多方合约的组合。在货到付款的场景中，参与方包括买方、卖方、货运方三方，其中卖方和货运方都可以以智能合约参与，而整个交易依然是原子化的。这在目前以太坊智能合约模式中是难以做到的，需要至少二个独立的智能合约调用，因而存在欺诈风险。

安全的关键在于用户不经手智能合约直接控制自己的资产。有人可能会说如果坚持这么做，很多 DEFI 应用就无法进行。如果张三不先把钱给智能合约，智能合约怎么能代表张三把钱借给李四？这种论点误解了控制权与所有权的差别。从法律上说，张三把钱给智能合约，转的是控制权而不是所有权，是控制未来将钱转给李四的权利。因此如果有一种机制能转移控制权而不转所有权，就依然能实现 DEFI 的目的。零熵中包含二种转移控制权而不转所有权的机制。

	目前的智能合约	明示合意智能合约
意思表达	转给合约的以太币；	任何通证都可以转给合约；

	合约可理解的调用参数	合约可理解的调用参数； 交易发起人想要的结果
执行	合约只要执行成功，用户必须接收结果	节点验证合约提供了想要的结果，若结果不符，交易失败
执行结果	存储在合约记录中	UTXO 输出，只有发起人可以解锁
安全性	合约钓鱼，合约程序错误，误解导致合约执行结果不符合客户预期；黑客攻击合约导致客户资产被盗	合约钓鱼，合约程序错误，误解均会被拒绝，不会导致用户损失；黑客不可能通过攻击合约盗取用户资产

明示合意智能合约和以太坊式智能合约的比较

5、土地通证

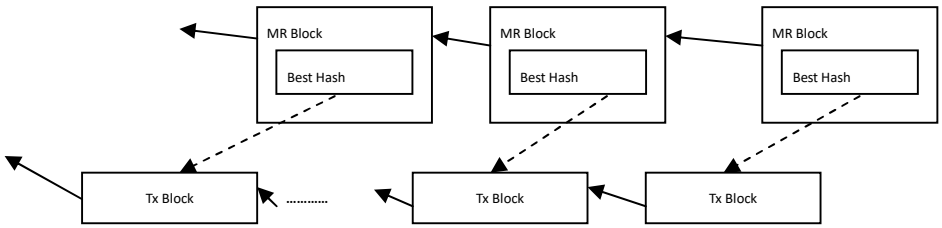
零熵中的价值可以不是数值形态，其中一种非数值形态的价值就是土地通证。在零熵中土地表达为一个经纬度为坐标的多边形。所有土地来源于创世区块中代表整个地球表面的多边形。多边形可以分拆和合并，矿工验证分拆前总多边形与分拆后的总多边形完全相同，没有增减、重叠。因此链中每个多边形唯一地代表一块土地。当然，也可以是海域。一个国家的边界线可能需要上百万个坐标，对于大型多边形的表示，零熵解决了有效表达和处理大型多边形及未知或待定边界的问题。土地通证可以附带权益信息，如所有权、承包权、经营权、产出权、抵押权等等。土地作为一种重要的资产，利用区块链技术对土地进行处理，扩大了区块链技术的使用范围。

6、零熵共识算法

区块链技术中一直存在一个所谓的三难困境（又称为不可能三角），指的是在区块链中分散性、安全性、可扩展性三者之中，提升一方性能必定以其它二方的牺牲为代价。三难困境源于区块链的单链式数据结构。区块承载着区块链的目标。传统的单链式数据结构中只有一种区块，却要承载有内在冲突的三个目标，自然会产生困境。零熵通过采用双链数据结构避免了陷入三难困境，实现了在不牺牲分散性和安全性的前提下无限可扩展性。

零熵由一个矿权链和一个交易链组成，矿权链记录谁获得了挖矿的权利，交易链记录区块链上的交易。矿权链采用工作量证明机制，工作量证明难度目标为 10 分钟，与比特币相同。交易链不使用工作量证明。矿工按照矿权链所记录的顺序依次产生预定数量（200 个）的交易链区块。由于在任何时刻谁有产生交易区块的权利都是确定的，因此无需以竞争性的方式决定合法交易区块，即交易区块不需要工作量证明，矿工签名就够了。因此可以以极高的速度处理交易。交易处理速度仅受限于节点验证打包交易的能力。

出于安全的原因，矿权区块包含产生该区块的矿工地址和一个交易区块的哈希值。矿权链中所引用的交易区块不能分属交易链中不同的侧链，不能前后颠倒。产生矿权区块需要工作量证明。由于引用关系的结果，矿权链因工作量证明而带来的安全性也传递到了交易链上，因此零熵中的交易有等同与比特币交易的安全性。



由于矿工必须先产生矿权区块然后才能获得产生交易区块的权利，因此任何时候都有一些其矿权区块已经在矿权链中，但尚未开始产生交易区块的矿工。这些矿工构成了一个等待队列。零熵用调整工作量证明难度的方式将等待队列的长度控制在 40 左右。这意味着当一个矿工开始产生交易区块时，他的权利已经被确认 40 次了，不可能被推翻。即零熵的交易链不可能因为二位矿工都宣称有权产生交易区块而出现侧链。因此除非有产矿权的矿工自己作恶，在同一高度签署了二个区块，否则任何交易区块一旦产生就是最终确认。

为阻却矿工双重签名，零熵要求矿工在产生矿权区块时提供ω币质押，为鼓励矿工多提供质押，零熵根据质押的多少调整工作量证明难度。如果真的出现了矿工双重签名的情况，零熵将没收质押的ω币用于赔偿用户的损失。赔偿额是交易费的 10000 倍。因此在零熵中，用户支付的交易费具有保险的性质。

质押只是为了阻却矿工双重签名。零熵并不依赖质押解决矿工双重签名造成的分岔。由于矿权区块必须引用一个交易区块，在出现双重签名造成分岔时，矿权区块只会引用到其中一个分岔中的区块，另一个分岔被舍弃。因此零熵用户也可以象比特币用户一样等待若干次矿权链的确认后再完成交易。对于质押不足以赔偿的大额交易来说，用户应当采用等待确认的方式。对于小额交易，一旦交易被记录用户可以视为最终，从而获得快速完成交易的好处。

零熵还采用调整工作量证明难度的方式激励矿工提高交易处理速度。具体方

法是：在矿权区块中，矿工可以报告其他矿工打包产生交易的速度。这种报告不是依据交易区块中时间戳来计算的，而是根据该矿工实际收到区块的时间来计算的。矿工产生矿权区块时，他的工作量证明难度会根据其他矿工所报告他的交易处理速度（除去最高和最低的 25%）的平均值和最近一段时间内所有矿工交易处理速度报告平均值之比而调整。因此能比其他矿工更快处理交易的矿工有更高的机会产生矿权区块。

自区块链技术出现以来，由于区块奖励远远大于区块交易费，矿工们将大量资源投入到提高哈希碰撞算力上，而不是提高交易处理速度。零熵一方面将交易费变成保险金，鼓励用户多付交易费。另一方面通过调整工作量证明难度激励矿工快速处理交易。因此矿工们会更好地平衡在提高哈希碰撞算力和提高交易处理速度能力之间的投入，使零熵发展成为一个高效的区块链。

7、扩展的行签名

在比特币中有一种单行签名，即交易输入中的签名所针对的是交易中该行输入和同一行输出的数据，而不是整个交易。通过这种方式可以一群人可以各自提交自己的签名，然后组合成一个交易。零熵对行签名进行了扩展，签名可以是针对交易中多行（最多四行，未来可以扩展至更多）的输入和输出数据。

用户通过交易的输出表达其对交易结果的要求，而这要求经常需要多个输出才能完整地表达，为了在一个交易中完整地表达需求，签名需要涵盖这些输出。如果用户需求超过四项，可以把多个行签名串联起来，后一个行签名包括前一个行签名的最后一行，而最后一行包括用户所提供的必要输入。

这种方式可以用于一种安全的交易所模式。这种模式无需客户将资产转入交易所，而交易所依然可以撮合交易。客户向交易所提交一个行签名的交易，输入是客户用于交换的资产，输出是验证交易中有用户希望得到资产的合约调用。这样的交易单独是不成立的。交易所将匹配的二个用户交易组合成一个交易，交易就成立了，而用户根本就不需要将资产转给交易所。

五、 研发进展

上述技术方案已经实现，采用上述技术的公链已经于 2020 年 7 月上线，已经产生了 1500 多万交易区块，用户可以通过社区网站（http://omegasuite.org）浏览区块和查看其它信息。相关技术的 4 项专利申请也已提交，并申请了国际专利。

六、 内置货币的发行

零熵主网包含其内置货币，Ω币（符号为ω）。一方面，Ω币作为奖励发放给矿工以促进网络安全，另一方面也面向投资人发行Ω币以获得开发和社区建设所需要的资金。Ω币的最小单位是毫（ħ），1ω = 100000000 ħ。Ω币挖矿奖励的发行模型如下：

最初每个交易区块可以获得 6ω的奖励。此后每过 42000000 个交易区块（大约是 4~5 年的交易区块数量），每个交易区块的奖励数量减半。直到每个交易区块的奖励数量为 1171875 ħ（大约 36~40 年后），则以后每个区块的奖励都是 1171875ħ，以补偿丢币损耗。因此首次减半前挖矿奖励总量为 252000000ω。前 40

年挖矿奖励总量约为 5 亿ω。

在挖矿奖励之外，零熵包含一个向投资者分阶段发行Ω币的智能合约。该合约在向投资者发行Ω币的同时按 50%的比例分别配发给社区开发团队和作为预留币。该智能合约发行Ω币的总量不超过 1.88 亿ω。