版本号：V1.0.0

SimpleChain

白皮书 Beta

简 单 上 链

SimpleChain Foundation©

2018.12.24

版权声明

摘 要

随着区块链在多年实践中的发展，它已然突破了原本的技术边界，而逐渐形成了产业化的影响力。在新数字经济的时代趋势下，我们看到区块链实践案例不断应声落地，与此同时，商业应用中的模式问题与技术桎梏也逐渐暴露。因此，上链（SimpleChain）理念应运而生。上链（SimpleChain）是一款以简单上链、共促共赢为设计理念的公有链。作为一项革命性的区块链应用基础设施设计，上链（SimpleChain）通过其灵活性、扩展性、稳定性、开放性和流通性的特点推动区块链技术与应用的前进与发展，以支持多元共识和性能要求来保障平稳安全运行，从而满足丰富的商业应用场景。

工作量证明机制作为区块链从比特币当中诞生以来的首个共识机制算法，以其长期的稳定性经历了时间的考验，也因此，上链（SimpleChain）的主链底层共识同样选择以独创的 PoW 算法运行，以确保分布式账本的一致和安全。节点客户端的提供也方便所有参与者自由成为上链（SimpleChain）的节点，并贡献自身的算力进行分布式账本验证。为确保整体设计的灵活性，主链上层被设计为可扩展的子链集，通过子链的定制化开发，上链（SimpleChain）可进一步承载丰富的区块链应用。单个子链的算法不限于 PoW，用户可根据需求设计其他共识机制、区块数据结构以灵活适应不同的场景应用，同时子链内部支持应用分片机制以满足开发者的交易性能需求。主子链结构赋予了上链（SimpleChain）充分的可扩展性。不断完善的配套工具让用户轻量接入、简单上链。

主子链通过数据交互紧密结合，不仅在技术层面能够同步区块链账本、支持跨链交易，还在激励层面构建了数字资产流通的经济模型。上链（SimpleChain）的原生数字资产被定义为 SIPC——通过主链 PoW 挖矿产生，用于记账激励和消费流通。SIPC 的流通总量与子链数量及子链内部对 SIPC 需求正向相关，预设合约可根据算法动态调节 SIPC 供应总量，满足用户对 SIPC 的需求并平衡资源价格。

为了构建开放透明、一致认同的分布式社区，开放性原则被写入上链（SimpleChain）的创世区块作为运行机制。上链（SimpleChain）的发起者和初始运营方为上链基金会——一个以推动上链开放生态繁荣为使命的非营利组织。基金会既没有预挖也没有自留任何数字资产，基金会第一年初始运营资金来自于全网矿工持续挖矿奖励中 5%的捐助，此后每年捐助的比例减半，直到社区完全自发运营。

上链（SimpleChain）致力于聚合社区全球研发力量，以兼容性与实用性并重，推动区块链技术的沿革与分布式数字经济生态的建立。

目 录

图目录

1 区块链现状与问题

1.1 多样式发展与较稳定的 PoW

自比特币白皮书中将区块链作为一种点对点电子现金系统底层技术[1]概念首次提出以来，区块链作为一种综合性技术架构已衍生出了多种类型的技术结构，从开放性程度上被分为公有链（Public Blockchain）与许可链（Permissioned Blockchain），许可链当中又可根据参与方的多样性分为联盟链（Consortium Blockchain）与私有链（Private Blockchain）[2][3]。

而从区块链核心的共识机制中，则经过演化形成了工作量证明（PoW）、权益证明（PoS）、代理权益证明（DPoS）、拜占庭容错（BFT）等不同类型的算法形态。PoW 机制在比特币“挖矿”过程中所造成了军备竞赛以及算力集中形成了能源的大量消耗。目前，比特币“挖矿”全年耗电量已超 64TWh，约为 33 亿美元的成本[4]，相当于比特币当中每一笔交易完成矿工确认的成本在 100 元人民币左右。大量的资源消耗使得 PoS 机制应运而生，PoS 使用算法来计算每一个节点所拥有的权益，并根据权益占比分配获得记账权的几率[5]。

由比特股所首次提出的 DPoS 机制则可以理解为现实当中的代议民主制，即每次共识之前事先存在代理节点，负责对全网交易进行签名验证。由于需要签名验证的节点数量较少，因此交易确认的效率会提升许多[6]。

追本溯源，较早的共识机制问题可以追溯到 Leslie Lamport, Robert Shostak, Marshall Pease（1982）[7]所提出的拜占庭将军问题，即在各方不可信环境中，在即时通信成本为零的情况下，多方是难以达成最终一致性的问题结论。论文中也提出，当不可信的参与方在 1/3 以下时，整个网络能够做到拜占庭容错（BFT）。拜占庭容错在发展过程中又进一步通过降低算法复杂度由指数级降低至多项式级，形成了实用性拜占庭容错（PBFT），提高了效率，能够达到每秒处理上千笔请求，从而在实际系统应用中变得可行[8]。

在主链当中使用 PoS 作为共识机制的方式日渐增多，如 PeerCoin 与 NextCoin 通过将持币时间与持币量等参数加入到共识算法中，实现了一定程度上不需要消耗大量计算资源的区块创建、奖励与延长机制。然而到目前为止仍然少有大规模主链 PoS 得以持

续运行，以太坊的 Casper 共识也尚未完成切换，因此其稳定性仍有待验证。PoS 需要用户实时在线，不然则可能在部分节点离线时，其他部分节点合谋伪造区块链历史记录，形成长程攻击[9]，此外，开放性的 PoS 共识在收敛速度上也并不稳定。DPoS 为机制的区块链虽然提升了收敛速度但并不支持验证节点的扩展，当节点数量增多时会造成性能效率降低。也因此，基于比特股历史发展而来的 EOS 提出了仅支持 21 个主节点的类联盟链结构。PBFT 则作为适用于联盟链的共识机制体系，需要启动区块链前即确定节点数量，且不支持共识进行过程中的节点增减，并且同样具有节点扩展性限制的问题，目前尚未完成过节点数超过 100 的链上共识实践[10]。

PoW 虽然消耗了大量的能源，但仍然是目前各类区块链中较为成熟的共识技术，经过了诸如比特币、以太坊、莱特币等大量规模性区块链的长期稳定性实践，并在容错性与激励机制上也有较好的体现，用户的动态加入与退出成为了 PoW 共识机制下区块链真正开放的基础[11]。

1.2 算力支撑过度与性能低效

PoW 作为区块链这项新兴技术中相对成熟、稳定的共识算法，在应用中也仍然存在着算力竞争与垄断的问题。以比特币区块链为例，当前全网已形成超过 30000P 每秒的哈希算力规模（BTC.com, 2018）[12]，而全球目前最尖端的超算系统 Summit 的秒算力是 122P（Top500, 2018）[13]，虽然超算所进行的是浮点运算，但在比特币区块链网络中，意味着即使全球前 500 的超算系统同时开机进行哈希运算，也难以达到 30000P 算力的一半，也就意味着难以从外部对比特币区块链完成 51%攻击。因此，比特币矿机算力的持续扩张，能源的持续消耗实际上已失去了意义，仅通过计算哈希值的挖矿方式也使得算力的扩张成为了纯粹的消耗。

然而在比特币区块链网络内部，算力分布的格局却存在着垄断的趋势。自 2012 年第一台比特币矿机诞生以后，不断升级的 ASIC 芯片超越了 PC 电脑的算力。矿机组成的矿池成为一个个比特币网络的“大节点”，权力趋于集中。《财富》（Fortune）杂志披露了某矿机商通过运营矿池、出售 AISC 矿机实现对比特币算力的集中控制，以及主导比特币硬分叉产生 Bitcoin cash（BCH）。不仅如此，分叉币的诞生直接与比特币争夺算力。根据钛媒体报道，2018 年初某矿机商在比特币挖矿专用 ASIC 芯片的市占率将近 8 成，占据绝对垄断地位，直接掌握着 30%左右的比特币全网算力。只要比特币

价格有利可图，算力大军仍在不断扩张和竞争。

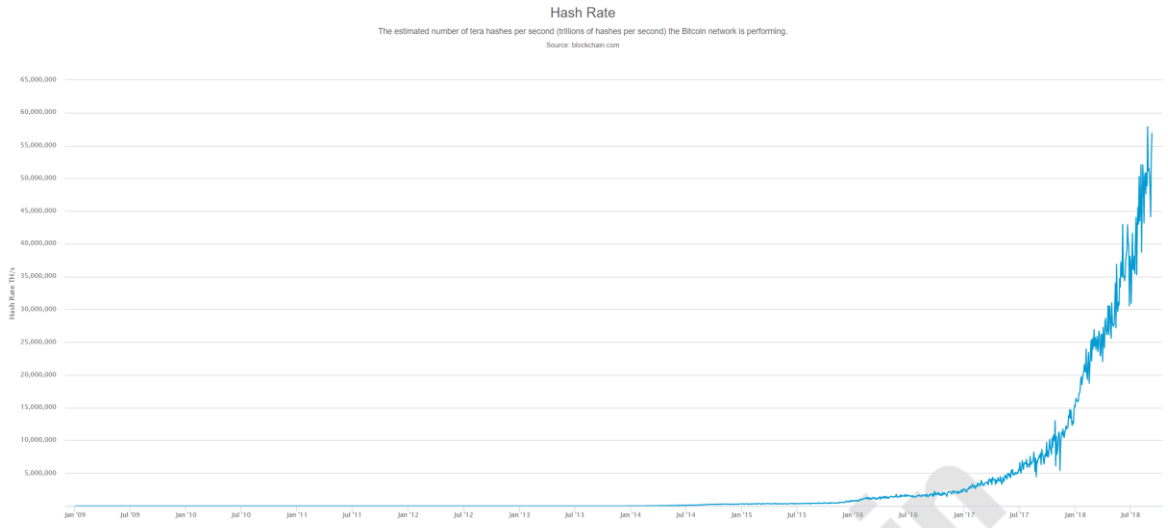

图 1 比特币区块链算力

行业已经逐渐形成共识，算力过度输出终将造成浪费，而不再是有效的工作量证明。我们知道，比特币挖矿是做一系列的哈希运算，输出大量算力得到的是一串无意义的数值，因此被斥为一种能源浪费。但并不是所有消耗大量算力的计算行为得到的都是浪费，例如人工智能。区块链提供的算力与人工智能所需算力本质上都是计算设备提供逻辑运行支撑的计算能力集合，但从结果来看两者显著不同。人工智能消耗大量算力经过训练、模拟形成的是一个逻辑事件的判断结果。因此我们希望能结合区块链与人工智能，将大规模算力输出与需求相匹配，形成有效工作量证明（EPoW）。

1.3 经济与社会激励的扩展与矛盾

随着区块链技术应用的规模扩展和场景深入，一些矛盾逐渐暴露出来，成为行业发展中亟待考虑和解决的问题。矛盾主要体现在四个方面：

1.3.1 内部发展方向矛盾

在区块链诞生以来位数不多这几年中，由于社区意见向左或利益纠葛，最终引起区块链分叉的案例不在少数。此外，各类面向垂直行业的区块链有着各自特点，能够全面满足各式应用需求的基础公有区块链屈指可数。

区块链圈里第一个有影响力的硬分叉应该是以太坊的分叉事件。以太坊上一个著名的项目 The DAO 由于其自身漏洞，导致黑客窃取了当时价值约 6000 万美元的以太币。

2016 年 7 月，以太坊开发团队通过修改以太坊软件的代码，在第 1920000 个区块强行把 The DAO 及其子 DAO 的所有资金全部转到一个特定的退款合约地址，从而“夺回”黑客所控制的 DAO 合约币。由于一部分矿工并不认同这个修改，于是形成两条链，一条为以太坊（ETH），一条为以太坊经典（ETC），各自代表不同的社区共识以及价值观。当以太坊发生了这次硬分叉后，产生了两条区块链。

BitMEX Research（2018）[14]统计了比特币共识分叉的历史事件，发现这些事件中至少有 3 次造成了明显可识别的区块链分叉。影响最大的一次硬分叉将比特币区块链一分为二，比特现金（Bitcoin Cash, BCH）成为一条新链。这次分叉起因是比特币社区对扩容方式的分歧。

1.3.2 不可能三角的存在

从比特币、以太坊到如今遍地开花的公链项目，从业者想找到的是一种能适应大规模商用的区块链。但区块链技术不成熟仍是行业现阶段面临的现实问题。2014 年文章《不可能三角形：安全，环保，去中心化》[15]中提出区块链技术存在性能的“不可能三角”，即去中心化、安全、环保三个方面无法同时满足。在 2018 年 4 月的“区块链之链智能之芯”论坛上结合当前流行的多种共识机制再次论述“不可能三角”观点[16]，即安全、效率（非计算性）、去中心化（计算性）三者之间不可共存，而现有的侧链或者分片技术介于去中心化和效率之间。

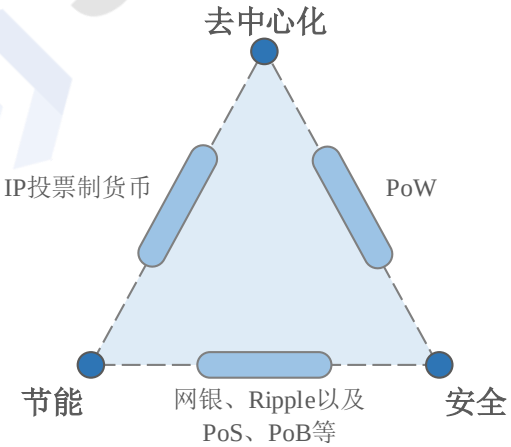

图 2 区块链的不可能三角

比特币区块链选择了去中心化和安全，但算力挖矿引致能源浪费的批评。同时带来的问题是牺牲了可扩展性。如果设计一个既环保又安全的密码学货币，要么本身是中心化架构或其去中心化架构不可维持，如 Ripple、PPcoin 本质上没有突破 PayPal、网银那

样的中心化验证机制。而 POS、DPOS 这样的“代议民主制”只是满足部分去中心的要求。EOS 为了达到百万级处理效率，只通过竞选 21 个超级节点来完成共识，牺牲了去中心化，但其实安全性也不能得到保障。然而牺牲安全的去中心化和环保没有意义。由此可见，试图在一条链上平衡三个因素的结果差强人意。

1.3.3 需求与成本的矛盾

公有链的特点之一是任何人都可以读写数据。网络上任何节点都可以参与挖矿来帮助见证和完成交易，挖矿需要矿工提供算力、存储等资源同时也产生电费成本，因此交易发起者需要向其支付报酬，这笔费用被称为手续费（矿工费）。从另一个角度来看，设置手续费门槛也是为了避免垃圾内容涌入公链，影响性能和用户体验。

比特币开创了区块链记账奖励的机制，通过链上代币发放激励节点完成交易，共同维护区块链网络。协作的综合成本仍比中心化系统低得多，且安全可靠。但由于每秒支持的交易量不多，链上需求的集中引发网络拥堵，手续费水涨船高。从图上看可以看出，比特币每笔交易的手续费经历过几次暴涨，2017 年的涨幅约 15 倍，高峰期完成一笔交易的成本近 150 美元。

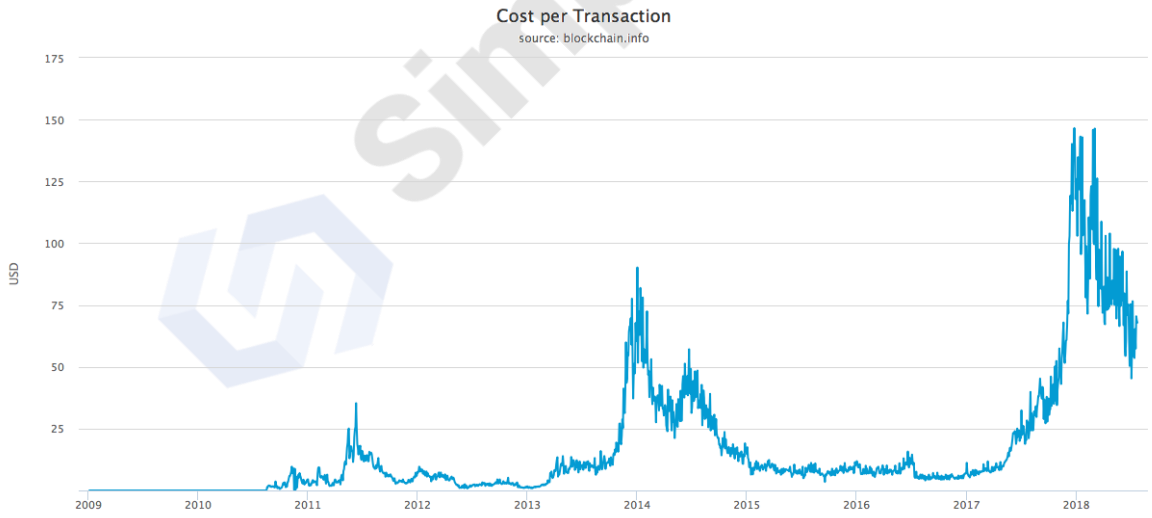

图 3 每笔交易的手续费

以太坊的手续费引入了 Gas 的概念。Gas 由两部分组成：Gas Price 和 Gas Limit。Gas Price（单位是 Wei，1ETH=10^{18}wei）指的是用户愿意为执行某个操作或确认交易支付的花费。Gas Limit 是用户愿意支付的最大 Gas 量。以太坊官网记录了历史每笔交易的 Gas Price，我们将其换算为美元单位，可以观察到手续费在 2017 年底和 2018 年 6 月经历了两次暴涨。原因或许可以跟两个时期的火热应用有关。

2017 年底，由于一款基于以太坊的区块链游戏 CryptoKitties 突然走红，占用了大量以太坊网络资源，致使以太坊网络一度瘫痪。用户为了达成交易不断推高 Gas Price，且当时恰逢加密货币牛市，ETH 价格屡创新高，以至交易手续费达到历史高位。2018 年 6 月，基于以太坊的 Fcoin 交易所玩出“交易即挖矿”的概念[17]，通过烧钱补贴和利润回购模式吸引用户，疯狂的交易量再度引发以太坊网络拥堵。因为此时 ETH 价格相比跨年时几乎腰斩，美元单位计价的交易费相对不高，但仍是非拥堵时期交易成本的 2-3 倍。

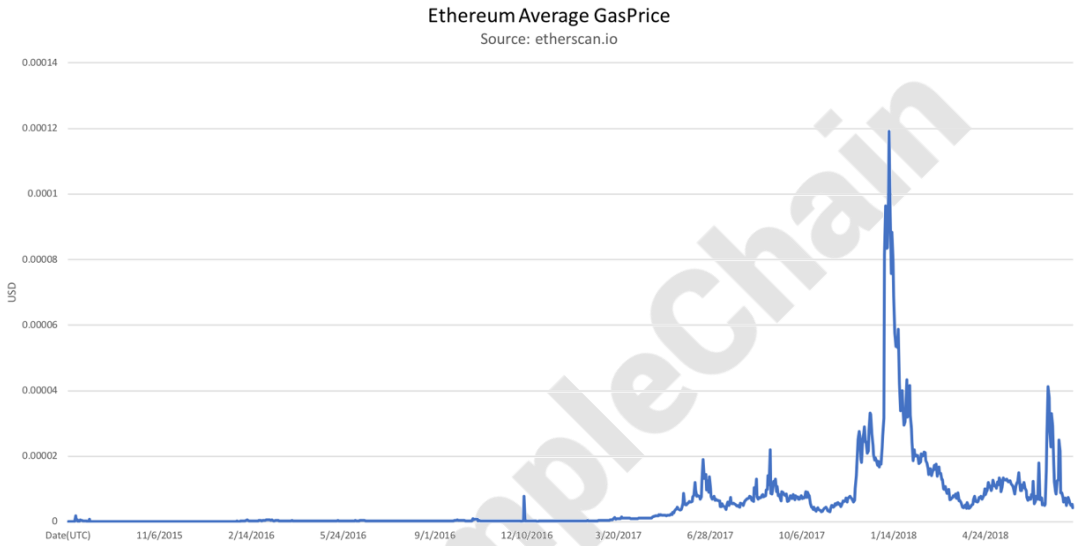

图 4 交易成本

相似的情况还发生在 EOS 区块链上。RAM（Random Access Memory）是 EOS 上应用开发所必需的存储资源。起初，RAM 是根据持有 EOS 代币的数量来分配的，但是持有大量 EOS 代币的人并不是开发者，就会造成有限的 RAM 资源浪费，特别是在面临公有链扩容和性能难题的当下。于是，EOS 基于 Bancor 算法创造了一个 RAM 交易市场，来促进 RAM 的流动性。市场投机行为造成 RAM 的价格短时飙升——13 天暴涨 54 倍[18]。毫无疑问对开发者来说，应用的开发和运营成本陡然增加，网络开发进度也可能因此减缓。这对尚未产生优质应用的公链网络来说未必有利。

在区块链刚刚诞生的时候，这种技术因为低成本优势饱受赞誉。然而我们在行业的发展中看到，由于性能限制无法快速满足大量交易需求，交易的成本被不断推高，反而使区块链的成本优势逐渐消失，并且抑制了应用扩展的积极性。对公链和应用开发者来说，如何打造“既受欢迎（创造更大经济价值）又使用通畅（避免成本过度扩张）的区块链网络”是一个重大议题。

1.3.4 创新与秩序的矛盾

早在 2017 年 4 月，The DAO 以时价约合 1.5 亿美元价值的以太坊，一举成为当时全球历史上最大的众筹项目。但由于智能合约的编写漏洞，存储在合约中的 ETH 被“黑客”所盗取，大量投资人利益受损。而按 The DAO 项目官方所陈述的，The DAO 应该是一个由不可伪造、不可停止、不可篡改的代码所完全支配的自由代币。也因此，使得 The DAO 的盗取从技术问题上升到了社会讨论，针对不可逆的区块链智能合约代码中所存在的漏洞来谋取私利，是否“合法”，又是否合理？以及，以太坊主网针对曾经号称不可逆的区块链进行硬分叉，帮助投资人找回被盗取的代币是否又符合区块链的原始逻辑？也因此，争议导致了以太坊的分叉，也让人意识到了“代码即是法律”的宣言与现实世界法律与道德的不兼容。

现有主要国家均以不同方式在法律条文中对数据、网络虚拟财产的保护做出了规定，体现了法律对虚拟资产的保护[19]。然而，当前主流公有区块链中的匿名性特点又使得资产确权成为了不可解，对权益的保护更是无从谈起。因此，区块链的新特点如何适应现有社会规则与法律，或推动其进步，也成为了区块链真实得以推动的基石。就如在区块链存证应用在司法中时，需要证明区块链技术用于存证时是在线状态并证明数据传递过程中不可能被污染等[20][2]，由此可见技术发展的快速与司法的滞后仍然是当前迫在眉睫的问题。

2 上链：化繁为简的分布式链网

2.1 SimpleChain 设计目标

SimpleChain，简洁基础的安全区块链协议框架与简易可用的公链创建平台，以机器共识建立可信网络。SimpleChain 充分吸收现有区块链项目的优点、解决目前存在的缺陷与问题、研发创新技术解决方案，目标为构建简洁易用的分布式链网，形成繁荣的应用生态。

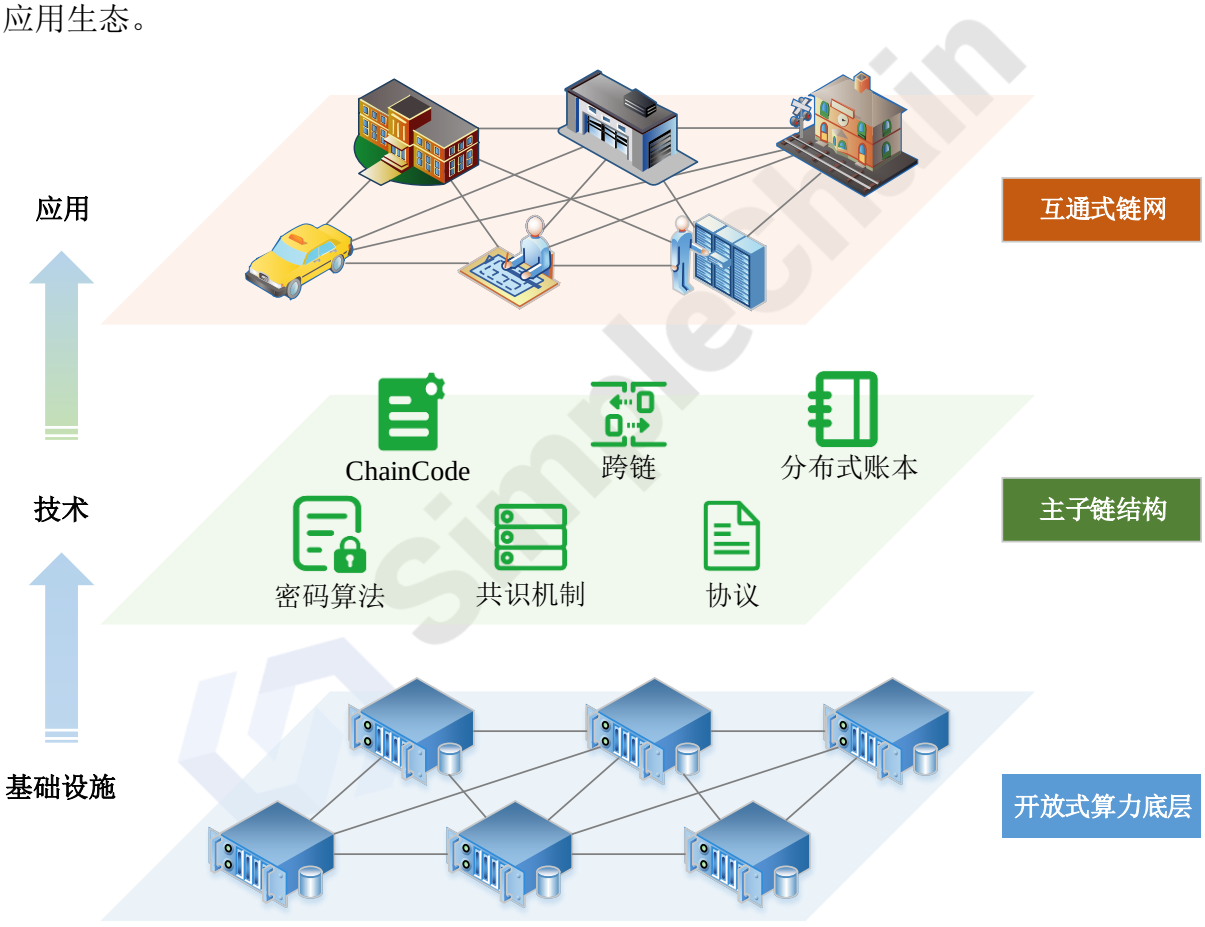

图 5 SimpleChain 分布式链网

SimpleChain 是一款以一主链多子链结构为设计理念的公有区块链，采用目前唯一经历过时间和规模验证的公有区块链共识机制工作量证明机制，并结合开放式算力底层，保证账本安全及激励持续。通过多层级的分布式价值网络设计，SimpleChain 支持多种业务场景的公有区块链部署与扩展。子链可根据业务需求设置适合自己场景的共识算法，通过跨链节点与主链形成双向锚定，与其他子链形成跨链交易，帮助子链在满足

每秒数千级别性能的前提下同时获得主链所提供的最终一致性。

2.2 SimpleChain 应用生态

SimpleChain 采用的主子链结构支持多种业务场景。对于子链项目，可根据实际需求选择适宜的共识算法，子链通过跨链节点与主链形成双向锚定，并与其他子链形成跨链交易。

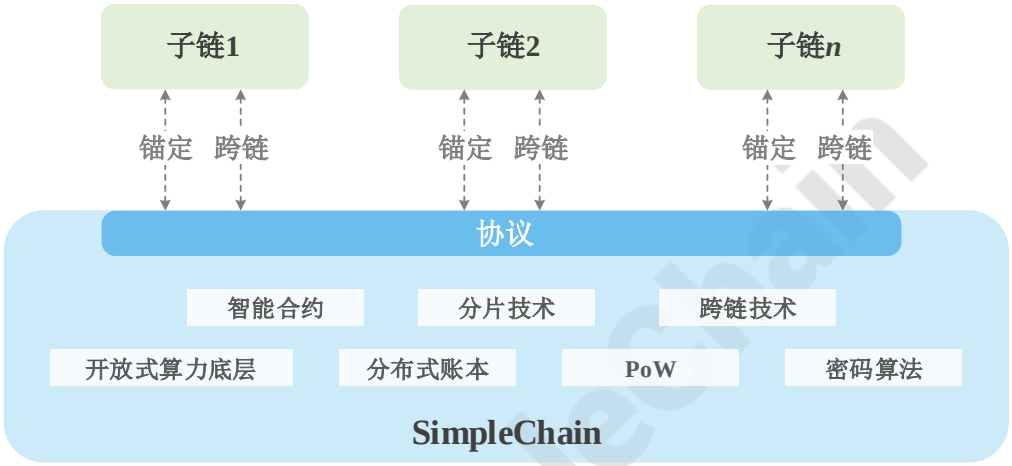

图 6 主子链结构

2.2.1 子链应用场景

SimpleChain 一主多子结构的链网生态在确保最终一致性的基础上，为多应用场景提供了高自由度的扩展支持。多类型的应用场景也增加了其生态的完整性，SimpleChain 已支持的子链项目涉及大数据、数字娱乐、奢侈品、不动产、稳定币、版权保护等多个领域，还链接了司法联盟链，为整个链网提供司法支撑。通过多行业分布式的数据交换和合规框架下的价值交换，形成良好、稳定的生态体系。

2.2.1.1 数据交易

在过去的几年中，互联网行业、金融行业、政府机关等都在不同程度的探索建设大数据交易项目，但这些大数据项目面临着各类问题，包括数据安全隐患、数据孤岛、数据质量低、流通方法不健全等问题，而政府大数据大多处于不公开状态，这些数据没有得到良好运用，未发挥其最大的价值。

利用区块链分布式、透明、可溯源等特点，在保护数据所有人隐私和合法权益为前提，以合规、安全的数据流通为基础，消除数据提供方的担忧，同时满足数据需求方寻找合规、正规数据的需求。通过区块链+大数据，将数据资产化，完成高效清算、结算和核算，激发数据交易的积极性，促进市场繁荣，突破数据孤岛，真正实现跨域连接的建立。

2.2.1.2 数娱游戏

传统游戏商店的发布模式中，游戏产品提供商与玩家都是弱势群体，寡头游戏平台以中心化的方式决定了玩家能够看到什么游戏，以及游戏能够获得多少玩家。中心化的管理使得游戏的生命周期越来越短，玩家与游戏之间无法匹配的现象成为限制当前游戏产业健康发展的顽疾。

游戏世界链（Game World Chain）通过建立在区块链上的游戏发布平台，实现游戏产品提供商与玩家之间点对点价值网络。游戏产品提供商可基于 GWC 发起游戏项目众筹，潜在玩家可对特定题材的游戏产品提案进行投资，以 GWC 提前换取游戏内资产的优惠奖励。游戏内资产统一作为链上资产进行管理，可设置锁定期。锁定期过后为犹豫期，犹豫期为游戏上线后的一段时间，玩家在此期间可按一定比例将游戏内资产换回 GWC。其他游戏玩家可根据游戏内资产与 GWC 的交易量判断游戏受欢迎程度，从而可对游戏产品提供商的水平进行评价，以数字价值为驱动，形成健康的分布式游戏产业生态。

2.2.1.3 钻石

钻石有别于与其他商品，难以达到统一定价，而钻石属垄断市场结构，价格透明度不足。与此同时，钻石市场缺乏流动性，因经常滞留在单边市场，无法以其真正市价转售出去。虽然存在钻石交易所，但大多是仅限于 B2B 交易，而在市面上交易的钻石，由于涉及的流程和工序较多，买家无法或很难辨别其品质及真假。

将钻石与区块链相结合，实现钻石仓单票据数字化，形成便捷、高效的数字钻石交易方式，完成传统钻石行业与创新型金融市场的链接，通过创新且安全的形式吸引传统钻石交易链中参与者、变卖钻石的持有者、需要避险的投资交易商等，由此汇聚更多钻石交易者，让这些参与者以安全稳定、透明公开的方式进行钻石交易和投资。利用数字

仓单票据交易还减少钻石流通的成本和造假的可能，持有者可随时提取钻石。

2.2.1.4 不动产

不动产是指依自然性质或法律规定不可移动的财产，如土地，房屋等土地定着物，目前有大量的人员在投资不动产，还有一些希望投资国外不动产，但在投资过程中会存在政策不明、流程复杂等问题，而在找第三方的过程存在手续费过高、信息不明确等情况。

Lunabay 是一个社区成员共建的全年龄养老社区，对社区成员个人不动产以及社区配套服务（产品）的全透明化、动态、精准管理，提升社区成员在全年龄阶段的生活品质，进一步形成全球最专业的全年龄养老服务社区。鉴于在全球范围内，不动产依然是大部分个人在整个生命周期中最重要的固定资产，Lunabay 基于区块链技术对不动产产权和使用权进行确权、认证和分配，能最大程度地平衡其社区成员在不同年龄阶段消费、投资和养老的综合需求。

2.2.1.5 稳定币

数字资产交易市场诞生以来，便捷安全可信的交易方式一直未能被找到。一方面，多数加密货币的波动性非常大，不利于支付和投资。因此从业者构建了锚定主权国家货币的“稳定通证”用于计价估值和支付。但目前市场上出现的几种稳定通证也存在问题，如抵押美元资产发行稳定通证但无托管和审计，存在信用超发、挪用资金、暗箱操作等风险。另一方，中心化的交易所安全性存疑，资产被盗、恶意爆仓等行为让投资者失去信心。

MintEx 依托于外汇投资服务经验，将外汇交易与数字资产交易紧密结合，打造安全可信的数字资产交易平台。MintEx 设计的稳定通证 Mint 锚定外汇资产，相应的资产存托在银行，流通中的 Mint 随资产总量变化而增减，从而构成了外汇资产-数字资产交易的连接器。

2.2.1.6 分布式算力

随着科技的发展，计算机随处可见，为人们的生活提供了巨大的便利。然而实际使

用过程中，若需要计算或存储大量数据时，则购买对应的服务器或者存储空间，由此存在成本和复杂性，同时无法对所需算力值进行准确的量化和评估。

在分布式算力子链项目中，用户可以根据自己拥有的权益获取对应的分布式算力，对于用户获取的分布式算力，可根据自己的需求进行操作，例如人工智能中数据训练等。通过分布式算力的权益化，使得算力分配更加合理和透明，满足用户对于算力的需求和应用。

2.2.1.7 版权保护

目前人们版权保护意识有所增强，但互联网技术的发展让作品复制和传播更加容易，使得数字盗版泛滥，很多作品在未经授权就被传播。与此同时，数字版权贸易日益频繁，版权授权需求量激增，传统版权交易方式具有过程复杂、交易成本高、交易效率低等特点，无法适应互联网时代数字版权贸易的需求。

区块链版权保护平台为互联网时代的版权保护提供有效途径和方式，可线上进行作品交易，平台将作品所有使用、传播等过程全部记录在区块链，有效对原创作品的版权进行保护，使其获得合法权益。除传统的作品版权外，还可将个人 IP 数字化，对个人 IP 的收益根据设定进行自动化分配，维护个人相关作品、肖像等内容版权的同时增加其价值，促进版权交易市场的流通。

2.2.1.8 数字鉴证

认定案件事实必须以证据为基础，只有获得真实、充分的证据才能保证准确查明案情。在传统证据收集过程中，会存在取证困难、时间长等问题。与此同时，随着科技发展，很多数据以数字化形式存在，而电子数据具有易复制、删除、修改等特点，导致证据收集存在更大的问题和困难，这也是使得司法工作过程缓慢、效率低的原因之一。

通过区块链与大数据有效结合，为现有司法体系的完善提供稳定支撑和执行辅助。利用区块链分布式、透明等特点，实现证据的快速获取和验证，形成司法信息同步协同，提高案件处理效率，避免数据孤岛，减少时间、空间的限制，顺应互联网时代的变革，推进司法创新。

区块链作为 P2P、分布式数据存储、密码算法、共识机制等计算机技术在互联网时

代的创新应用模式，本质是具有“货币+票据+凭证+财会”功能的新型架构，使得其可结合于不同场景，但由于不同的应用场景对于链上交易的验证与确认频率、链上数据格式与容量、性能及开放性等要求各不相同，为确保公链平台的最大兼容性以及不同应用所在链上交易的有效隔离，一主多子的 SimpleChain 将成为分布式应用开发者易用、安全的开发平台。

2.2.2 SimpleChain 入口

2.2.2.1 浏览器

为 SimpleChain 用户提供的区块链浏览器包括上链浏览器和节点浏览器。

上链浏览器是浏览 SimpleChain 链上信息的主要窗口，每一个区块所记载的内容都可以从上链浏览器上进行查阅，其中包含了主链原生数字资产与链上发行的其他各类资产账本数据，通常数字资产用户会使用区块链浏览器查询记录在区块中的交易信息。上链浏览器支持用户查询主链与各条子链的内容。可查字段包括区块高度、区块哈希、挖矿难度、区块大小、出块时间、交易手续费、交易地址等。

节点浏览器是为SimpleChain 节点用户开发的可视化管理面板，提供了活跃节点数、出块时间、全网算力、挖矿难度、交易手续费等信息，帮助节点用户了解自己节点以及全网其他节点的连接状态与延迟情况，以便于优化网络环境。对于挖矿节点，使用节点浏览器有利于其监测自身所处的网络连接通畅程度，对于一般节点则能够监测自身交易被区块链网络确认的及时程度。

区块链浏览器是用户与开发者最为直观地认识 SimpleChain 的入口，以可视化的方式将各类数据进行展示，开源的浏览器更接受社区进行的二次开发，从而更好地监控 SimpleChain 的运行与发展。

2.2.2.2 客户端

SimpleChain 为用户提供简单上链的客户端软件。用户可以通过客户端创建和管理账号、同步账本并查询相关信息，开启区块链之旅。通过部署客户端成为节点后，用户能够发送和验证链上交易，也可以通过客户端可视化地部署智能合约，进而轻松创建自己的区块链应用。矿工用户通过客户端即可参与挖矿、管理矿工的行为。客户端是用户

最为直接地参与成为 SimpleChain 区块链分布式网络成员的重要工具。

2.2.2.3 跨链资产钱包

区块链钱包是用户管理数字资产的工具。为方便用户管理 SimpleChain 主链数字资产与链上的其他各类通证，团队已开发一款多币种数字资产钱包 ChainBox，具备查询、存储、转账、交易等功能，适用于苹果、安卓等操作系统的移动端智能设备。未来将持续对 ChainBox 优化升级，支持更多功能和更多种类的设备。

2.2.2.4 区块链存证取证平台

一直以来电子化的数据难以确认唯一性和真实性，造成了数字商品盗版侵权严重、隐私泄露难禁难查等问题。SimpleChain 的子链（保全链），利用区块链可溯源不可篡改的特征搭建了一个基于区块链的电子数据服务平台——保全网，为用户提供可信电子凭证服务、在线取证服务和版权保护平台。这个应用的优势在于用户数据可以不依赖于公司存在，而被永久地保存在区块链上。保全网的产品流程和证据效力已经率先获得中国司法体系的认可（2018 年 6 月 28 日），有效降低了用户确权、自证与维权的法律成本和周期。

保全链将为 SimpleChain 的区块链产品（子链或应用）提供中国司法保障需求的接口和工具，支持其它子链或应用对接，帮助区块链用户存证、取证和维权。因此，保全链作为 SimpleChain 的子链，能够对所有 SimpleChain 上其他子链提供鉴证服务，使得上链生态的链上交易在获得区块链链上节点的共同验证外，还能够获得外部司法体系的保证与认可。保全链作为 SimpleChain 创世子链应用，也将成为传统中心化数据实现简单上链的关键入口。

3 上链通证流通与激励机制

本章节首先说明 SimpleChain 经济模型设计的原理，然后对主链通证（SIPC）及 SIPC 与子链通证之间的关系进行分析，最后介绍 SimpleChain 总量与调整方式。

3.1 通证发行与流通

3.1.1 经济学模型设计说明

3.1.1.1 通证说明

1、通证属性

货币被定义为一种提高交易效率的媒介共识[21]，具有四个功能：交易的媒介、记账的单位、储存价值和延期支付的标准[22]。并且，货币属性因经济体系兴衰而演变：商品经济的兴起衍生出金属货币；金权[23]经济的兴起衍生出金属代用货币[24]和信用货币；共享经济的兴起衍生出超主权货币[25]。目前，全球还处于金权经济为主的市场体系，信用货币效率最高[19]。

基于金权经济为主的市场体系，通证不过是一种标记使用权的数字商品或有价证券，并非货币。SimpleChain 产生的通证来源于挖矿，根本产生于算法。算法产生的通证经历的要素流通过程如下图：

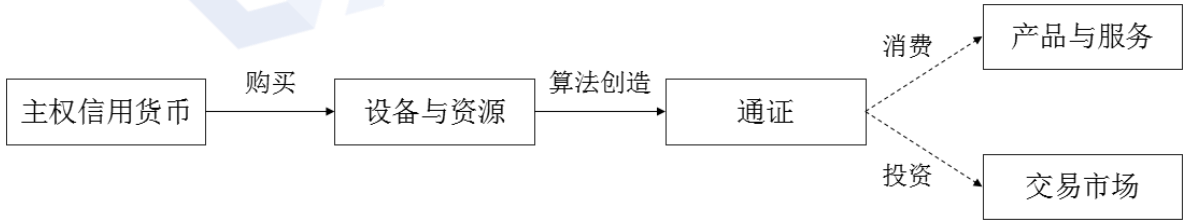

图 7 算法形成通证的过程

在数字经济视角下，主权信用货币成为新增通证的一种外部输入源。而智能合约如央行般发行通证，通证可被用于消费和投资。因此通证的状态主要有三种：1）以数字形式被持有；2）通过消费行为进行交易；3）兑换为货币退出流通。

2、主子链通证说明

（1）主链通证 SIPC

主链通证作为整个生态系统中的媒介通证，以挖矿的方式获得，使用于链上交易或是合约调用，在运算过程中燃烧 SIPC。同时，子链稳定通证以及非稳定通证与 SIPC 通过对价的方式产生关系，换句话说，SIPC 的价值由这两类子链通证共同决定。

（2）稳定通证

稳定通证通常是一种在一定时期内价格相对稳定的区块链通证。在整个主链生态圈内，稳定通证既可以通过兑换主链通证 SIPC 来支付相关费用，也可以通过兑换非稳定通证的方式进行投资。稳定通证由稳定通证团队发行，并锚定指定法币，主要具备支付功能。而稳定通证的发行方式可以自由选择，发行方可以通过法币准备金 1:1 存入商业银行的方式发行，也可以通过抵押实物（如钻石、黄金等）或者数字资产的方式发行。其中，数字资产又根据生态圈进行划分，对于主链生态圈内的数字资产（主链通证 SIPC 以及子链通证）通过链上智能合约的方式进行托管，而主链生态圈外的数字资产（如 BTC 等）则托管于第三方平台。由于稳定通证具有高稳定性，决定了主链对其的优先验证权，这也让其对主链拥有更高的贡献价值权重。

（3）非稳定通证

非稳定通证的价格自由浮动，类型包括功能型通证、商品型通证、证券型通证等。非稳定通证由非稳定通证团队发行，是主链生态的重要支撑者，既具有流通属性也具备存储功能。随着子链非稳定通证项目的不断接入，越来越多的应用场景对用户开放，这在提升用户量的同时也吸引了主链算力向子链应用中的发展。而非稳定通证项目又连接着真实的商品市场，实现商品以虚拟数字化的方式进入到生态系统之中，从而打通行业之间的壁垒，让其在进行跨链流转的同时逐步完善主链生态。

（4）主子链通证的流通关系

在 SimpleChain 体系下，通证主要分为主链通证、子链稳定通证以及子链非稳定通证三类。而稳定通证以锚定信用货币、实物资产或数字资产而发行，这让货币、稳定通证和非稳定通证形成了相互可兑换的流通关系，如下图所示：

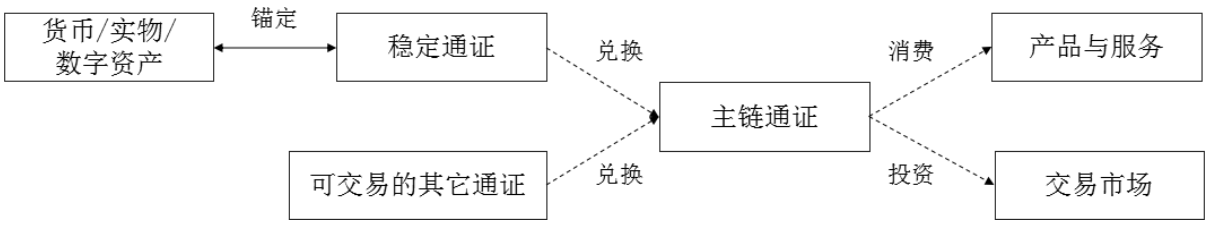

图 8 货币、稳定通证与非稳定通证的经济循环

其中，稳定通证符合货币定义和功能，非稳定通证来源于区块链项目的“信用创造”。而在这样一种 P2P 流通体系下，“银行”中介无需存在，借贷关系和信用保证更加直接。货币理论在相应条件下仍然成立且值得参考。

3.1.1.2 通证的供需模型

1、通证（需求）数量论模型

一般情况下，由于通证在区块链经济体系中所提供的流动性特点与货币类似，因此可选择参考货币模型，从货币的交易规模以及交易货币的流通速度角度，可以得到费雪（Fisher）交易方程式[26]，如下所示：

$$MV_t = P_tT$$

其中，M 表示货币数量，V_t 表示货币的交易流通速度，P_t 表示价格水平，T 表示交易规模，P_tT 表示所有交易的价值。更进一步地，假设交易规模 T 等于实际总产出（即主链总产出，由子链稳定通证以及非稳定通证相关因素共同决定），用 Y 表示。同时假设流通速度 V_t 较为稳定（用户形成一定的交易习惯），那么流通速度 V_t 可以看作为一个常数 $\bar{V}$，则从资产角度，可得到剑桥派的货币数量论，如下所示：

$$M_d = kP_tY \quad (k = \frac{1}{\bar{V}})$$

那么，映射到区块链当中，通证需求 M_d 与实际交易量 Y、价格水平（即以主链通证为标价的其他子链通证或链上数字资产的价格水平）P_t 成一定比例关系。若进一步将影响因子细化，则可以得到基于各影响因子的通证数量论模型[27]，如下所示：

$$\frac{M_d}{P_t} = f\left\{Y_p, e_t, t_c, s, v_t, \frac{1}{P}\times\frac{dP}{dt}, i_t, u\right\}$$

其中，M_d 表示通证需求，P_t 表示价格水平，与 M_d 正相关；Y_p 表示用户的收入水平（包含所有链上或链下资产中可用于支配购买通证部分），与 M_d 正相关；e_t 表示稳定通证实物或金融资产抵押物预期名义收益率（即抵押物在链下金融体系中的收益率），与 M_d 正相关；t_c 表示交易花费的成本（包含链上交易手续费以及链下资产兑换为链上资产的费用部分）；s 表示通证平均换手率；v_t 表示通证流通速度；$(1/P)\cdot dP/dt$ 表示价格预期变化率（即预期通货膨胀率，包括因为子链需求增长的主链通证增长率），与

M_d 负相关；i_t 表示抵押比率变化函数（以下简称“比率”，比率高则代表发行通证所需的代价越高），与 M_d 负相关；u 表示其他影响货币需求的变量，如用户的投资偏好等，与 M_d 的关系不定。

进一步地，提取出关键因子：收入水平、交易花费成本、比率，再根据著名的鲍莫尔-托宾模型（Baumol-Tobin Model），并将持有通证总成本最小化可以得到基于交易动机的平方根公式[28]，如下所示：

$$M^* = \sqrt{\frac{Y_p}{2} \cdot \frac{t_c}{i}}$$

其中，M^* 为最优通证平均持有量；Y_p 为通证持有人的收入水平，与 M^* 成正相关；i 为比率，与 M^* 成负相关；t_c 为交易花费的成本（即交易所需消耗的 SIPC 量）；每月交易一次的月平均通证持有量等于月收入的一半，即 $Y_p/2$。因此，通证的交易需求与收入水平同方向变动，与比率反方向变动。

2、短期比率规则模型

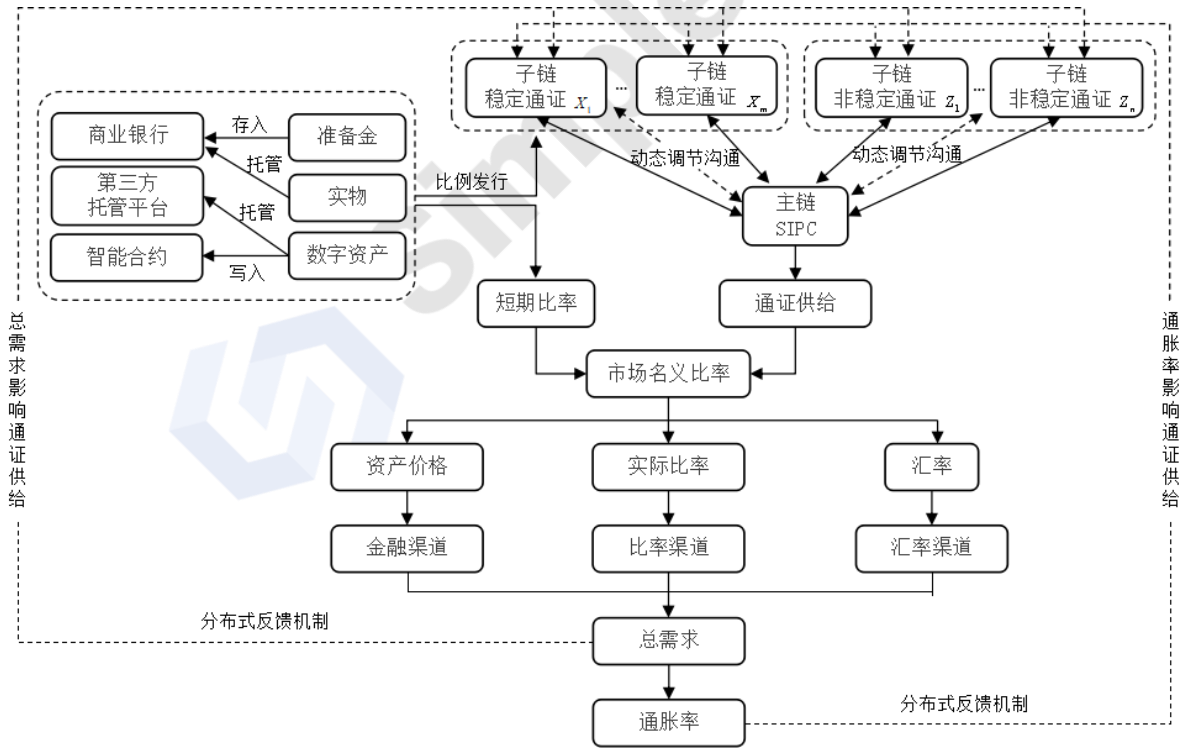

图 9 通证供给动态调节分析图

主链通证 SIPC 的需求及价值由子链稳定通证及非稳定通证决定，即根据子链需求来动态调节主链 SIPC 的供给。如上图所示，短期比率作为稳定通证发行的重要影响因子，对主链通证供给调节起关键作用。资产价格、实际比率以及汇率又通过金融、比率、

汇率三大渠道对总需求产生影响，而总需求的旺盛又形成了通货膨胀的压力。但基于主链生态的分布式反馈机制，总需求及通胀率会同步传输至各子链，并通过与主链的动态流通来进行供给调节，所以通货膨胀率又在很大程度上作用于比率的波动。因此以比率(i_t)为工具的通证供给调节方程式可写成一般形式：

$$i_t = f\left(i_{t-1}, R, \pi_t^*, X_t^*, Z_t^*\right)$$

其中，$f(\cdot)$表示主链通证供给调节函数，R表示平均短期实际比率，包括通过主链通证资产抵押形成的子链通证流动性所带来的价值增益率，π_t^*表示主链通证实际通胀率与目标通胀率之间的差，X_t^*表示稳定通证产出缺口（即实际稳定通证产出与潜在总需求之间的差），Z_t^*表示非稳定通证产出缺口（即实际非稳定通证产出与潜在总需求之间的差），i_{t-1}用来捕捉通证供给动态调节的平滑特征。

又根据泰勒规则，可以将短期比率规则模型进行如下表示：

$$n_t - \pi_t = R + \alpha(\pi_t - \pi^*) + \beta(\frac{X_t - X^*}{X^*}) + \gamma(\frac{Z_t - Z^*}{Z^*})$$

其中，n_t表示名义比率，π_t表示通货膨胀率，$n_t - \pi_t$表示实际短期比率，π^*表示通货膨胀目标值，$\pi_t - \pi^*$表示通货膨胀目标值的偏离值，R表示平均短期实际比率，X_t表示稳定通证的实际产出，X^*表示稳定通证的潜在总需求，$(X_t - X^*)/X^*$表示稳定通证产出缺口比率（即实际稳定通证产出与潜在总需求之间的比率），Z_t表示非稳定通证的实际产出，Z^*表示非稳定通证的潜在总需求，$(Z_t - Z^*)/Z^*$表示非稳定通证产出缺口比率（即实际非稳定通证产出与潜在总需求之间的比率），α、β、γ分别表示通货膨胀率偏离目标值和稳定通证以及非稳定产出缺口冲击的权重。因此，当产出缺口比率为正且（或者）通货膨胀率偏离值为正（即通货膨胀率高于设定的目标值）时，可以对短期比率实行溢价；反之亦然。

3、主链通证供给模型

主链通证 SIPC 的供给量在不同时期会有所波动，主要受到某时期子链通证的流通量影响。又根据上面的短期比率规则模型，主链通证的供给模型的一般式可以表示为：

$$M_s(t) = f\{(X(t), Z(t), i(t)\}$$

其中，$M(t)$表示主链通证供给函数（即t时期通证供给量），$X(t)$表示稳定通证产出函数，$Z(t)$表示非稳定通证产出函数，$i(t)$表示以比率为工具的通证供给调节函数（即

主链对通货膨胀率变动的反应函数）。

更进一步地，供给函数[29]又可以表示成:

$$M_s(t) = X(t)Z(t)(P_{t-1}PP_{t-2})^{-q}$$

其中，$M_s(t)$表示t时期主链通证供给量，$X(t)$表示稳定通证产出函数，$Z(t)$表示非稳定通证产出函数，P_{t-1}、P_{t-2}表示t-1、t-2期的价格水平，q表示主链通证对通货膨胀率变动的反应系数。而再对上式两侧取对数并求导，可以得到下式，如下所示：

$$m_{s_t} = x_t + z_t - q(p_{t-1} - p_{t-2})$$

其中，m_{s_t}表示t时期主链通证的增长率，x_t表示t时期稳定通证的增长率，z_t表示t时期非稳定通证的增长率，P_{t-1}、P_{t-2}表示t-1和t-2时期的通货膨胀率。而因为稳定通证的高贡献价值权重，我们可以认为$x_t - q(p_{t-1} - p_{t-2}) > z_t$，即主链通证增长率$m_{s_t}$主要受稳定通证的影响。又鉴于稳定通证锚定法币而具有的高稳定性，对于主链通证的消耗需求，随着稳定通证子链的不断加入，可以满足主链长期稳定发展的预期。

3.1.1.3 节点制衡原理

目前（截止 2018 年 9 月 3 日），比特币的全网算力已经达到 52.29 EH/s，也就是说，若以每台矿机 13.5T 来计算，那么每台矿机出块概率为 380 万分之一。因此，随着全网算力的指数增长，solo 挖矿的出块概率也越来越低，用户也逐渐向矿池协作挖矿转移。正如中本聪所论述到的，当网络成长到大规模时，每个节点都将会是巨大的服务器集群[30]。所以 solo 挖矿向矿池协作挖矿的转变可以说是自然发展的结果。

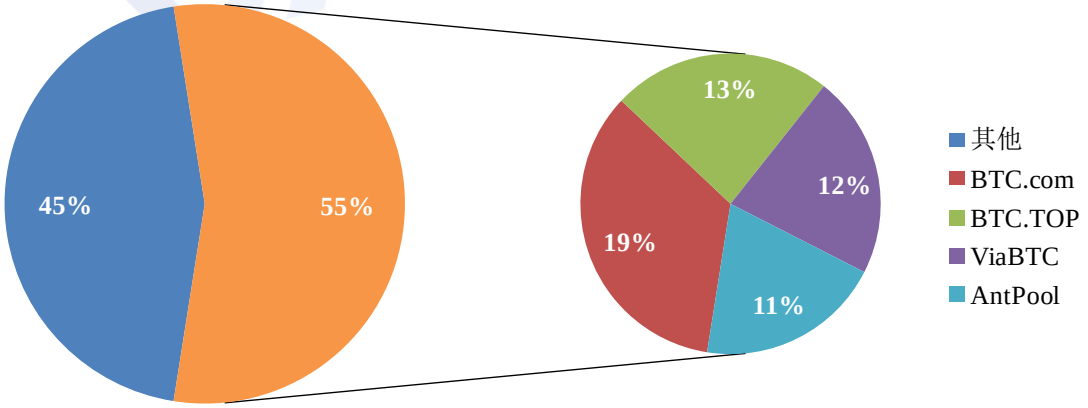

图 10 BTC 矿池份额图

比特币发展至现阶段，如上图（BTC 矿池份额图）所示，全网超过 50%的算力被

集中在了前四大矿池之中。虽然算力趋于集中化，但仍然分散于各节点之中，且单个矿池节点算力值也未超过全网的 25%。换句话说，BTC 已经形成相当数量且互相制衡的高效节点，并由这些专业化的服务器集群来运行打包区块的矿池全节点[31]。不可否认，对于算力集中的结果是可以预见的，并且高效节点间会形成相互制衡的关系，以此来促进网络生态的健康发展。

以比特币矿池算力为例进行分析，因算力集中而形成的节点制衡原理显露无疑。由下图中的散点图分析来看，近一年来，前四大矿池每个月（较前一个月比较）的算力占比波动情况基本维持在 2%以下，最高也未达到 6%。也就是说，高效的矿池节点算力已经形成了一定的规模，且能持续稳定住其持有的份额以达到互相制衡的效果。

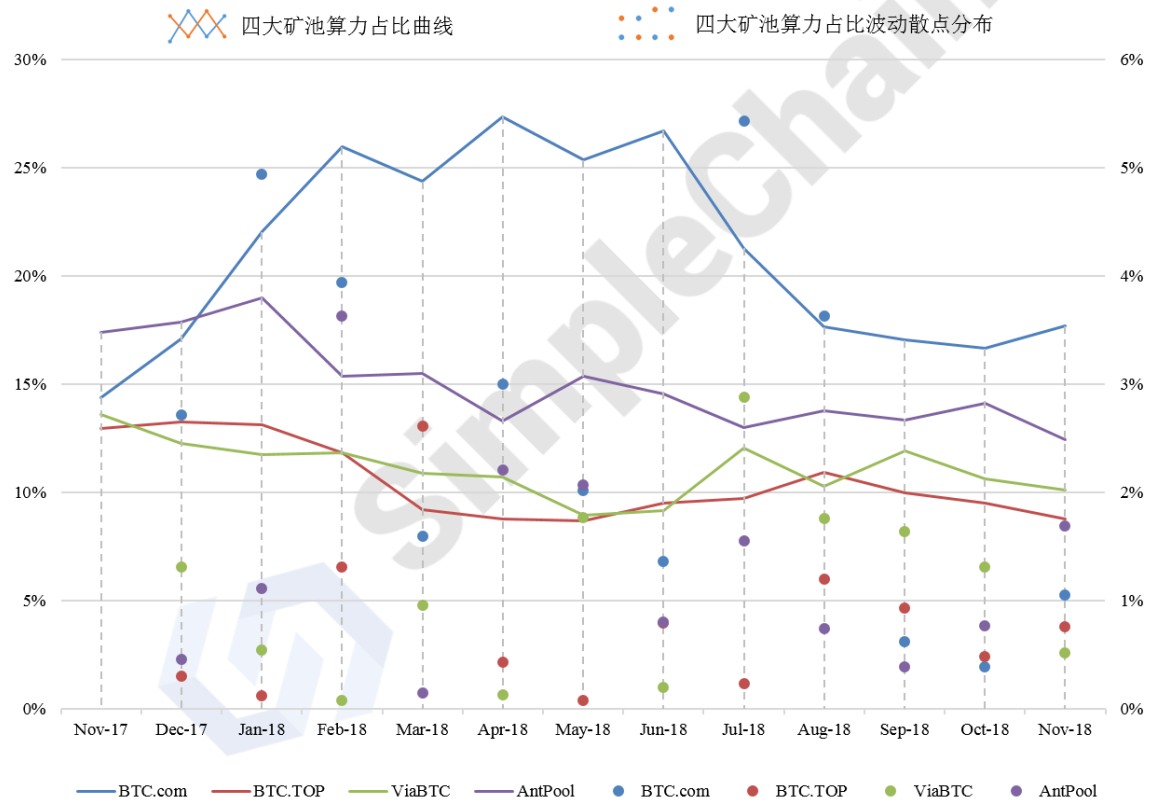

图 11 四大矿池算力占比/波动（月）分布图

假设全网算力已经形成特定的市场规模且处于平稳发展阶段，我们可以忽略其微小的波动率，那么在短时间内无论是矿池算力的占比情况或是 solo 挖矿的占比情况均可视为定值，即成功挖取区块概率保持不变。那么，从统计学角度分析，假设挖取每个独立区块的成功（$X=1$）概率为 $p\,(0\le p\le 1)$，失败（$X=0$）概率为$1-p$，那么随机变量 X 服从伯努利分布，方差可以表示为 $p(1-p)$。则根据 SimpleChain 预设的出块时间（12s），即平均每分钟出 5 个块，以每小时统计分析，可以得到挖矿回报的方差为

$60\times5\times p(1-p)$，期望回报为$60\times5\times p$，可以得到相对标准偏差为：

$$s=\frac{\sqrt{60\times5\times p(1-p)}}{60\times5\times p}\text{（可简化为}\frac{1}{\sqrt{60\times5}}\times\sqrt{\frac{1}{p}-1}\text{）}$$

由上述公式可以发现，用户所控制的全网算力占比越高，相对标准偏差越小，风险越小。所以对于用户投资来说，选择加入矿池，相较于 solo 挖矿，一方面可以减少挖矿回报的方差从而降低风险性，另一方面也避免了运行全节点的麻烦，用户只需运行轻量级 SPV 节点即可[32]。当然，在考虑风险性的同时，各大矿池的回报率也是用户需要考虑的一大要素。由上图中的折线图分析来看，BTC.com 在各时期的算力占比较其余三大矿池都有所优势，但其波动性也最大且到后期优势不再明显，其根本原因是矿池的信任度问题。当矿池节点拥有了大比例的算力，中心化的程度也就越高，对于回报分配越不可控，所以用户对矿池节点的信任度自然会有所降低，带来的算力波动也就越明显，用户的回报率也就越无法确定。但这恰好能让矿池节点之间维持住平衡，也解决了算力过度集中化的问题。总的来说，进入到矿池协作挖矿时期后，节点的制衡需要大量用户来共同维护，而用户可以根据回报-风险比值来对矿池节点进行选择，即挖矿回报与相对标准偏差的比例，可以表示为：

$$\frac{F(h)}{S(p)}=f(p,h,w)$$

其中，p 表示算力占比因子，h 表示矿池的信任度因子，w 表示影响回报-风险比值的其他因子。$F(h)$ 表示 h 为主要影响因子的回报函数，即挖矿回报主要取决于矿池节点本身的信任度 h，且当算力占比达到一定程度后信任度会随之降低。$S(p)$ 为相对标准差函数，表示风险率主要取决于算力占比 p，且与 p 负相关。所以在对矿池节点进行选择时，用户可以通过分析回报-风险比值来选择合适的矿池节点，比值越高代表投资越佳。当然，用户还能根据投资组合的方式来调节算力投入比例，即通过接入不同的挖矿节点来获得最高的回报比例。这样一来，用户也可以将风险分散化，进一步提高收益率。而对于挖矿节点来说，用户的多样性选择也稳定了自身的竞争力，最终达到节点间相互制衡的效果。

相同地，对于 SimpleChain 而言，所有发行的 SIPC 均由挖矿产生，所有的挖矿节点都根据原始设定的算法运行，通过全网的统一性来保证节点间的公平竞争性，以此推动相互制衡的挖矿节点的形成。初期，SimpleChain 会先对原始的 SIPC 出块奖励算法、难度调整算法等进行设定，而随着 SIPC 被逐渐挖出，其产量函数 $f_1(x)$ 如下图所示。对

于后期子链项目的加入，区块奖励函数 $f_3(x)$ 会与区块奖励参照函数 $f_4(x)$ 进行对比，通过动态调节来适当提升区块奖励值以适应子链需求。同时，为防范用户数的突然暴增以及全网算力值的指数增长，全网会进入到如下图所示的难度快速提升期，根据难度调整函数 $f_2(x)$ 对难度系数进行提升，以此保证 SIPC 产量的稳定增长。总的来说，通过全网算法的统一设定以及动态调节来保证节点间的公平竞争，以良性的竞争挖矿方式保证全网的动态均衡性，推动形成基于高效节点的健康网络生态。

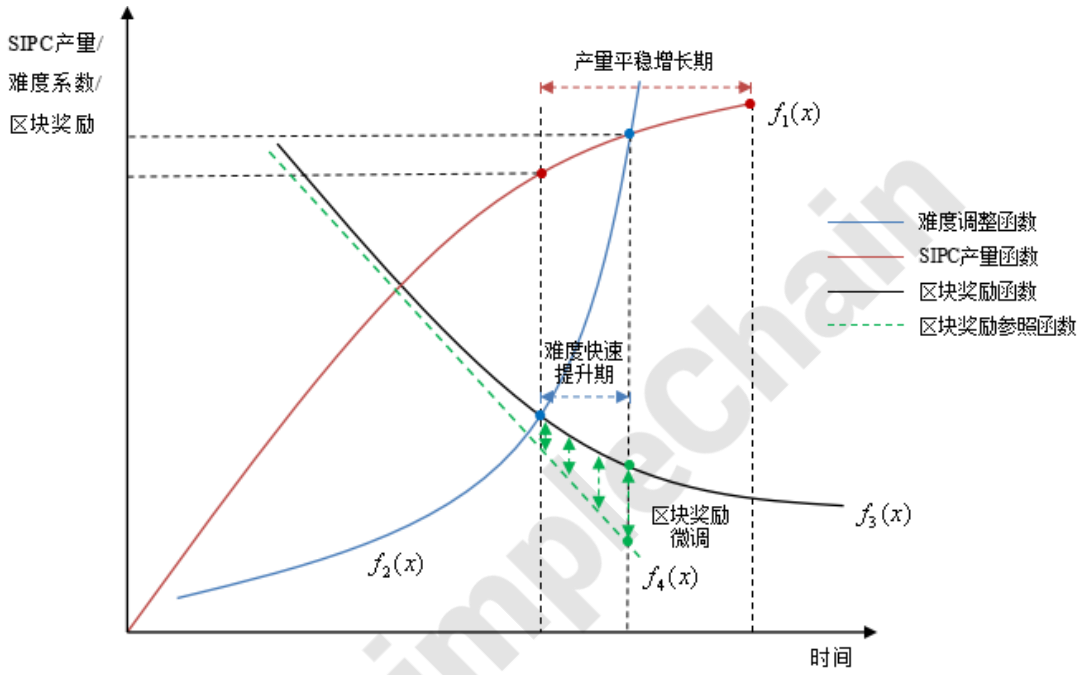

图 12 SIPC 函数图

3.1.2 多链通证机制分析

3.1.2.1 主链通证 SIPC

主链通证 SIPC 可用于子链生态建立、发展、正循环需要消耗的费用。

3.1.2.2 SIPC 总量动态调整

SIPC 的总价值等于各子链价值之和。

设价值为 W，主链有 $A_1, A_2, \cdots, A_n$ 共 n 条子链，对主链价值贡献权重分别为 $C_1, C_2, \cdots, C_n$。则有：

$$W_{SIPC} = \sum_{i=1}^{n} W_{A_i} * C_i$$

其中，W_{A_i} 表示主链 A_i 的价值，$W_{A_i} > 0, i = 1, 2, \cdots, n$；$C_i > 0, i = 1, 2, \cdots, n$。

SIPC 总量动态通胀的设计目的有二。

其一，适应新的子链项目加入 SIPC 生态链。

当新的子链项目加入主链时，主链价值提升，交易需求增加，此时需要动态调整 SIPC 的总量以满足交易需求。

类似交易方程式

$$MV = PY$$

其中 P 代表物价水平，Y 代表总物品，M 代表货币数量，V 代表货币流通速度。相对应 SimpleChain，Y 为链上总需验证的数据量，P 为验证单位数据量需要消耗对应 SIPC 价值，M 为 SIPC 总量，V 为链上一个 SIPC 流通速度。

假设子链数量为 n 时，链上总需验证的数据量为 Y_n，SIPC 的流通速度为 V_n，需要消耗的 SIPC 价值为 P_n；则当子链数量为 $n+1$ 时，链上总需验证的数据量为 Y_{n+1}，SIPC 的流通速度为 V_{n+1}，需要消耗的 SIPC 价值为 P_{n+1}。当有子链加入主链时，主链总价值提升，链上总需验证的数据量也会增加，因此有以下推理：

1、子链加入后，链上总需验证的数据量增加，即 $Y_{n+1} > Y_n$；

2、根据交易方程式 $MV = PY$，可以推出：

$$M = \frac{PY}{V}$$

3、为尽量确保链上手续费 P 和 SIPC 的流通速度不会有太大波动，则 $P_{n+1} \approx P_n$，$V_{n+1} \approx V_n$，而 $Y_{n+1} > Y_n$，则可以得出 $M_{n+1} > M_n$。

通过上述推理可知，实际中需求的通证总量会有提升，故 SIPC 需要微通胀。

其二，通证微通胀，持有者从增值角度考虑会优先选择购买子链相关产品和服务，这样可刺激子链产品和服务交易速度稳步提升，从而使子链更健康的发展。

3.1.2.3 SIPC 消耗机制

根据每笔需主链验证的交易容量大小（kb/tx）设定 SIPC Price，主链矿工根据 SIPC Price 排序确认。

SIPC Price 由两个因子决定。

第一， 交易容量大小；

验证的交易容量越大，消耗的算力资源越多，需要支付的价格越高。这是由交易自身消耗的无差别算力决定的。类似商品的价值；用公式表达为

$$y_1 = kx$$

其中 y_1 为交易容量价格， k 为常量， x 为验证的交易容量大小。

第二，矿工完成交易的实际时间。同类型的交易，当前交易消耗的时长越多，下一次交易对应的价格需要调整的越高，这是由主链矿工的自由选择决定，类似市场选择。一个交易长期无人问津，说明它消耗的交易费和估算的交易费有一定的偏差，导致矿工不愿接受。此时提高交易价格可以刺激矿工接受此交易。同理，当某交易被矿工快速验证完成时，说明此交易价格高于了市场价格，实际消耗的算力小于此交易的成交价，利润比较高。用公式表达为：

$$y_{n+1} = y_n * \frac{t}{t_e}$$

其中 y_{n+1} 为下一次预设的市场价格， y_n 为当前价格， t 为实际交易时间， t_e 为常量。

综上所述，交易的市场价与 y_1（交易容量价格）成正比，与 t（上次消耗的时长）成正比，与 t_e（交易的预期时长）成反比。

交易的排序规则遵从竞价排序，价高者排序靠前，保证有急需交易需求的能被优先处理，而对交易时间需求没那么紧急的用户拿到相对实惠的成交价格。

交易容量价格决定初始价格，迭代公式决定第 2 笔到第 n 笔交易价格。配合竞价机制，3 者共同决定了交易验证定价及排序。

3.1.2.4 稳定通证机制

主链矿工优先验证稳定通证子链，确保 SIPC 与稳定通证对价为先。

SIPC 生态环境建立之后，主链之下会对接多个子链。SIPC 作为主链，需要一定的稳定性，为子链的稳健发展提供必要的保障和支持。

子链因自身天然属性不同，会导致后天的稳定性不同，根据其相对稳定性，将子链分为两大类，稳定通证子链和非稳定通证子链。

此时主链价值和子链价值重新细分。设 W 为价值，子链分为两类。A 类，稳定通证子链 m 个，分别为 $A_1, A_2, \cdots A_m$ ，对应主链贡献价值权重分别为 $C_{A_1}, C_{A_2}, \cdots, C_{A_m}$ ； B 类，

非稳定通证子链 n 个，分别为 $B_1, B_2, \cdots B_n$，对应主链贡献价值权重分别为 $C_{B_1}, C_{B_2}, \cdots C_{B_n}$。则有：

$$W_{SIPC} = \sum_{i=1}^{m} W_{A_i} * C_{A_i} + \sum_{j=1}^{n} W_{B_j} * C_{B_j}$$

主链优先验证稳定通证子链，可以使 SIPC 价格与稳定通证子链价格有更强的正相关，从而使 SIPC 的价格与稳定通证子链的通证价格趋势保持一致。稳定通证子链的通证自带稳定属性，例如钻石币、黄金币、石油币等，优先验证稳定通证子链，从而使 SIPC 获得稳定性。

具体的实现方式如下：

主链交易验证的价格由三层参数组成

第一层：根据交易容量大小设定的价格参数。此参数设为 i。

第二层：SIPC 平台为稳定通证和非稳定通证设定排序价格参数，此参数设为 j。

第三层：用户愿意为每 kb 交易容量买单额外付的价格参数，此参数设为 k。

设某交易需要验证的容量大小为 x，则排序成交价格

$$y_M = x * i * j * (1 + k)$$

主链矿工验证交易所得为

$$y_N = x * i * (1 + k)$$

举例，假设稳定通证交易 A 和非稳定子链交易 B 需要主链验证。

其中 A 验证的大小 x_1=5kb、B 的大小 x_2=5kb；

假设 i=10，A 系数 j_1=1.2、B 系数 j_2=1.1。

A 的用户额外支付的 k_1=10%，B 对应 k_2=10%

A 在主链的交易排序价格设为 y_{M_1},则有

$$y_{M_1} = x_1 * i_1 * j_1 * (1 + k_1)$$
=5*10*1.2*（1+10%）
=66

B 在主链的交易排序价格设为 y_{M_2},则有

$$y_{M_2} = x_2 * i_2 * j_2 * (1 + k_2)$$
=5*10*1.1*（1+10%）
=60.5

由于 $y_{M_1} > y_{M_2}$，因此优先处理 y_{M_1}。

A 在主链的交易验证奖励设为 y_{N_1},则有

$$y_{N_1} = x_1 * i_1 * (1 + k_1)$$
$$=5*10*（1+10\%）$$
$$=55$$

B 在主链的交易验证奖励设为 y_{N_2},则有

$$y_{N_2} = x_2 * i_2 * (1 + k_2)$$
$$=5*10*(1+10\%)$$
$$=55$$

由以上可得稳定通证子链项目和非稳定通证子链项目提供的交易费用相同时，稳定通证的交易被优先验证。即，主链矿工优先验证稳定通证子链，确保 SIPC 与稳定通证对价为先。

3.1.3 SimpleChain 通证总量与调整方式

SimpleChain 的主链通证 SIPC 均通过挖矿产生，在主网上线时整个 SimpleChain 网络开始运行，同时产生 SIPC。

在子链未加入时，SIPC 的总量恒定不变，若子链加入，SIPC 总量会根据子链进行调整。在子链未加入时，SIPC 的总量为 C，假定 t 时间（单位：秒）出一个区块，第一阶段每出一个区块奖励 SIPC 数量为 m，每隔 T_s（单位：秒）奖励数量减少，对应衰减因子为 μ，则在没有子链的情况下 SIPC 的总量为：

$$C = \frac{T_s \cdot m}{t \cdot \mu}$$

根据当前 SimpleChain 的技术情况并考虑到后续生态的发展，各参数的值设定如表 1 所示。

表 1 SimpleChain 值设定

SIPC 总量	出块时间	初始奖励量	衰减时间	衰减因子
1.0512×10^8	12 秒	20	1 次/年	50%

通过上述设定值可得出，SimpleChain 的出块时间为 12 秒，初始出块奖励为 20 个 SIPC，每一年（即 365 天）奖励减半一次，在没有子链的情况下 SIPC 的总量为 1.0512×10^8，故每阶段出块奖励 SIPC 和挖出 SIPC 的总量如图 13 所示。

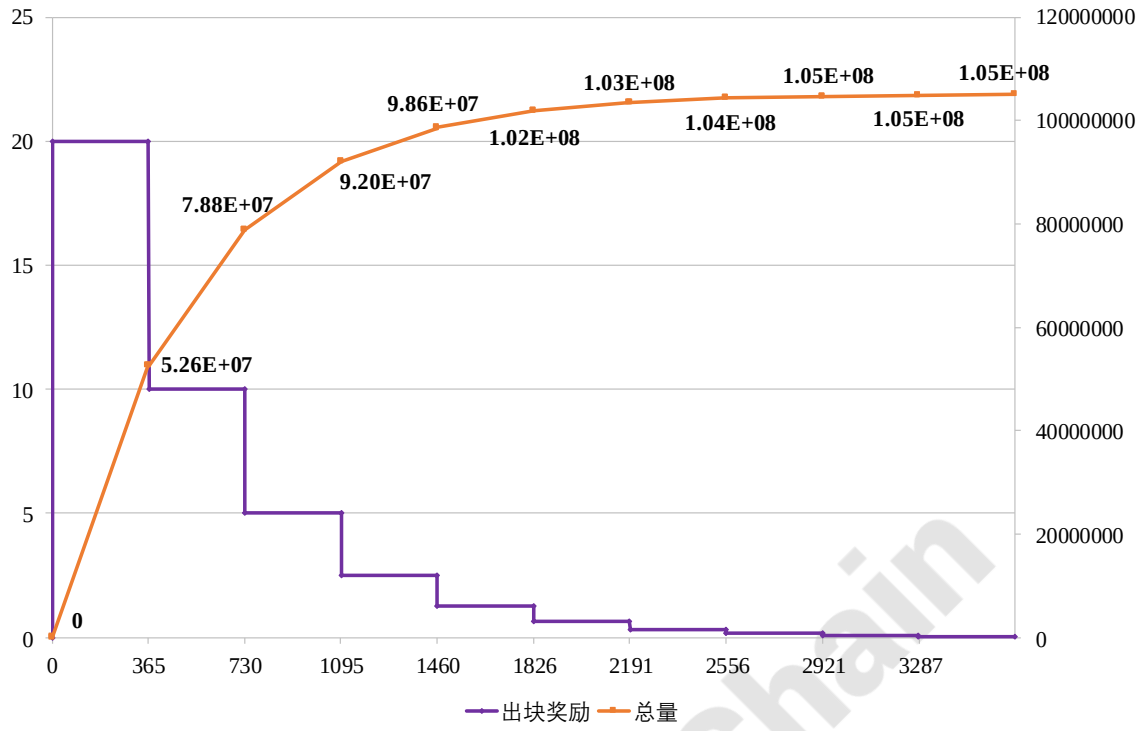

图 13 出块奖励 SIPC 和挖出 SIPC 总量

在子链加入后，SIPC 的总量会有相应的调整，即 SIPC 的总量会增加，增加量根据子链的类型、通证量和子链价值等决定。所谓子链类型指的是子链是否存在通证（某些情况下联盟链或私有链不存在通证），通证量是子链中通证总量，而子链价值指的是子链接入时通证的单价。

假设 SimpleChain 接入 n 条子链，ξ 表示是否存在通证（ξ=0 表示不存在通证，ξ=1 表示存在通证），第 i 条子链的通证总量为 c_i，子链接入时该通证的单价为 u_i，对应当时 SIPC 的单价为 U_i，则加入 n 条子链 SIPC 的增加量为：

$$C_{add}=\sum_{i=1}^{n}\left((1-\xi_i)\cdot c_i\cdot\alpha+\xi_i\cdot c_i\cdot(\beta+\frac{u_i}{U_i}\cdot\gamma)\right)$$

其中，α 表示子链不存在通证情况下子链对主链的影响参数，β 和 γ 分别表示子链存在通证情况下子链通证总量和子链价值对主链的影响参数。

3.2 生态激励设定

3.2.1 基础分布式账本激励

传统复式记账是以经营主体单点视角出发的记账机制，能够有效对内部账务中涉及

多个账户的的进出、收支等进行核验管理。然而在经济活动越发高频小微的当下，复式记账的滞后性与单点特性则对于宏观经济活动中的账目流通形成了限制。异步的记账与报账机制使得会计与审计成为了一项高度消耗经营主体成本的活动，而为了获得与之相应的激励回馈，则出现了“假账”、“小账”等作弊行为，以从税收的逃避中维持传统记账机制的持续。

区块链以全网账本状态共享与共验的形式，将原本属于经营主体自身的工作分散到了整个网络，将成本分摊的同时也以记账者通证激励的模式将激励也相应分摊，从而将维护账本的成本控制在账本网络本身当中，而不需要从外界额外获得激励进行维持。此外，时间序列的链式账本数据结构，也使得区块链成为了宏观层面的整体可追溯账本，穿透、全面的账本体系构建出了完整的经济运行路径。

基于工作量证明机制的 SimpleChain 向所有为链上账本提供记账服务的节点以其付出的工作时间与计算资源为计量，进行通证 SIPC 激励。基础激励的提供，也将推动节点在记账过程中记录、验证与叠加整个分布式系统的数据状态。

3.2.2 开发者社区与激励

为更好地推进区块发展和应用生态环境的建设，在公链发展中，我们设定了针对开发者的激励协议，希望通过奖励 SIPC 的方式感谢支持和帮助 SimpleChain 发展的开发者们。

对于代码贡献激励主要为智能合约的开发，激励协议是根据智能合约的优质度 Q 来判定应给予的奖励 R，而智能合约的优质度由调用和使用该智能合约的地址决定，影响的因数包括地址的影响度排名 I、影响因子 α 和活跃度 A，地址的影响度和活跃度越高，对应的影响因数值越大。

激励协议按照时间 T 为周期，奖励设为 M。为尽量实现激励的公平化，地址需要满足 $\alpha>0$ 且 $A\geq\lambda$（λ 为活跃度限定值，根据实际情况进行设定）才算为有效地址。在某个周期，共 T 个智能合约，并有 S 个有效地址调用了智能合约，智能合约 C 的优质度为 Q_C，该周期有 N 个有效地址调用了智能合约 C，则智能合约 C 可获得的奖励 R_C 为：

$$R_C=\frac{Q_C}{Q}\cdot M=\frac{Q_C}{\sum_{t=1}^{T}Q_t}\cdot M=\frac{\sum_{i=1}^{N}(S-I_i)\cdot\alpha_i\cdot A_i}{\sum_{t=1}^{T}Q_t}\cdot M$$

在实施过程中，为更加实用化，激励协议会根据实际情况进行调整和优化，最大程

度上促进 SimpleChain 发展。

除上述针对智能合约开发者的激励外，对于 SimpleChain 技术提出合理建议、发现问题并提出相应解决办法的技术人员，在对其贡献价值评估后也会给予相应的奖励。

3.2.3 节点扩展激励

SimpleChain 设定的节点激励根据链上节点种类进行计算，主链上包括普通的验证节点，子链包括子链验证节点，而为促使跨链交易将设定跨链节点。主链上普通的验证节点将完成主链上的记账，根据主链上采用的 PoW 机制，将获取出块奖励和记账交易的交易费；子链验证节点的奖励根据具体子链采用的共识机制和设定经济模型来计算；跨链交易节点是为了提供安全且正确的跨链交易，其同步的数据包括主链信息和子链信息，因此获取的出块奖励和跨链交易的交易费用。

为确保跨链节点的正确执行跨链交易，因此跨链节点数量和节点的选取必须更加严格，还会实行交纳保证金，若提供虚假交易，将被扣除保证金并取消节点资格。

4 上链主子链技术架构与拓展

SimpleChain 子链可根据场景需求选择适宜的共识机制，而为了确保整个链生态体系的稳定发展，主子链采用分片多层机制，并设有欺诈认证以惩罚矿工的作恶行为。本章节对主子链架构进行简要说明，并概述研发内容和计划。

4.1 主子链架构

4.1.1 子链可选共识

为适应各类行业的应用需求，SimpleChain 的子链采用多共识机制，即子链可根据实际需求选择合适的共识机制。SimpleChain 主链采用成熟的 PoW 机制，而子链内部节点仅负责内部共识，通过主链验证节点作为连接，实现各类共识机制特性的有效利用。由于目前提出的很多共识机制还在探索阶段，可能会存在不可预测的问题，采用子链可选共识的方式不仅可满足不同场景的需求，还能将子链的一些不成熟共识算法进行边界限定，主链对子链进行安全维护的同时避免子链的问题对主链产生影响。

4.1.2 主子链分片多层机制

4.1.2.1 主子链结构

SimpleChain 主子链同构，主链和子链的每个区块均包括若干个分片，主链分片包括本链交易分片和子链锚定分片，而子链分片包括本子链交易分片及主链与本子链相关的锚定分片。链上的区块包含若干个分片 slot，矿工按照 QoS 算法选择分片插入区块的分片 slot 中，在保证本链服务和锚定服务可用性的条件下达到最大 TPS。

为确保主链的轻量简洁，主链上不做大量的数据同步，仅作为全局账本维护机制。因此主链和子链结构采用类 DAG 的方式，会使用共识分片（网络分片、交易分片、状态分片）。在子链分片中，为确保信息流通和安全，会根据实际需求和情况进行合理的存储分片的管理和分配。SimpleChain 的分片技术会持续推进和研发，计划首先实现子链交易的分片打包，然后在此基础上完整实现子链分片功能提升 TPS。

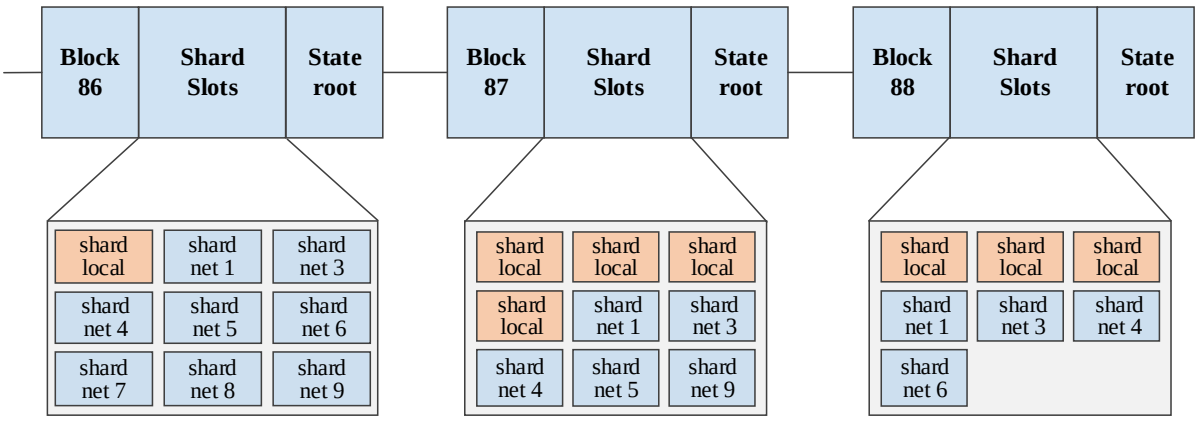

图 14 主子链结构

4.1.2.2 跨链转账交易

SimpleChain 跨链转账交易中跨链交易分片由锚定矿工生成，而主链与子链之间交易具体包括五步，如图 15 所示。

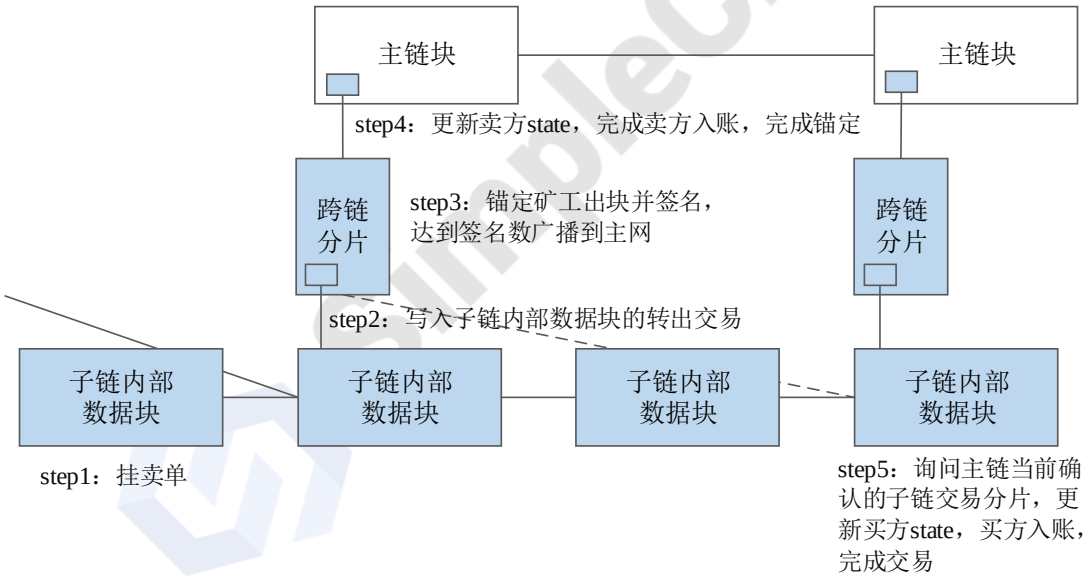

图 15 跨链转账交易步骤

在跨链转账交易中，主链和子链的操作均包括两个阶段，具体过程描述如下：

（1）子链用户提交跨链交易上链后，首先锁定通证（子链两阶段提交第一阶段）；

（2）其他用户提交购买交易（主链两阶段提交第一阶段）；

（3）锚定矿工匹配跨链交易产生的跨链交易锚定分片，由主链矿工验证后插入主链区块，并更新跨链交易主链部分状态（公链两阶段提交第二阶段）；

（4）子链节点作为主链的轻节点，通过默克尔证明确定锚定信息，并无条件更新跨链交易子链部分状态（子链两阶段提交第二阶段）。

跨链转账交易满足最终确定性，如果子链未按照约定更新跨链交易子链部分状态，锚定节点不会为对应的分叉生成锚定分片，因此，所有锚定在主链上的跨链交易最终均会被确定。与此同时，SimpleChain 主子链具有主从性，即便在主链临时分叉的情况下，任意一条分叉的主链与其锚定的子链上的跨链交易也满足原子性，最终被多数节点认可的分叉上的交易被确认。

4.1.2.3 锚定矿工的选择

设定每 n 个块为一个时期，在每个时期前，公钥地址为 PK_u 的锚定矿工 u 缴纳一定保证金加入矿工池。假设每条子链选择固定参数 K，时期 x 所有块的默克尔哈希值为 $H(x)$。在时期 x 即将结束前期，通过 $H_1\left(H(x),K,PK_u\right)<\mu$ 的方式为 x+2 时期选出各自子链的锚定矿工，其中 $H_1()$ 为哈希算法，μ 为设定的阈值。

为尽量避免和抑制欺诈现象的发生，SimpleChain 设有欺诈认证机制，任何人都可以通过欺诈认证去举证锚定矿工的作恶行为。若挑战者发现欺诈账户为 X，对应的锚定及锚定矿工签名为 hash1 和 hash2，举证过程如下：

1、挑战者质押一定保证金，要求对 hash2 签名的锚定矿工给出 hash1—>hash2、X 账户数据变更的默克尔证明及相应交易签名；

2、在一定时间内锚定矿工未能给出相应的证明，则该矿工将被除名，挑战者将获得一部分对应矿工的保证金，并将对应锚定块设为错误块；

3、若锚定矿工给出需要的证明，则挑战者将损失保证金。

4.1.2.4 主子链价值安全性

1）子链价值安全性

对子链数据的篡改仅在子链矿工与锚定矿工的联合作恶的情况下发生，锚定矿工对于节点较少、易受攻击的子链进行数据和价值保护。

2）主链价值安全性

主子链间的价值转换由市场决定，而子链矿工与锚定矿工的联合作恶必然会影响子链价值，导致主子链价值兑换率的改变。主链的价值依托于主链本身的价值及各子链间的流动价值。锚定矿工作恶将损失质押的通证，并由于具有较高价值的子链因矿工的逐利加入，作恶成本随子链的价值递增。对于主链来说，单一子链的作恶对主链价值的风

险较小。

4.1.2.5 锚定矿工签名最小化

为提升锚定效率并解决扩展性问题，在后续研发中计划采用 Schnorr 型多重签名技术，实现签名最小化。

所谓数字签名[33]，是类似于纸上的普通物理签名，用于鉴别数字信息的方法。数字签名只有信息的发送者才可以产生而其他人无法伪造的一段数字串，由此不仅能够验证信息的完整性和真实性，还可证实信息来源。在实际生活中，会存在多个签名者对消息进行签名的情况，为此 1983 年 Itakura 和 Nakamura 首次提出多重签名的概念[34]。后续研究者们基于不同数学难题提出了各类的多重签名方案，但相应的会存在签名长度随签名人数的增加直线增长的问题，且方案存在安全性问题。2006 年 Bellare 和 Neven 基于 Schnorr 签名方案提出了相对更加实用和安全的多重签名方案[35]。

Schnorr 数字签名方案诞生于 1991 年 Schnorr 发表的名为《Efficient Signature Generation by Smart Cards》[36]的论文，该方案是基于离散对数 DLP 困难问题，安全性相对较高。Schnorr 签名体制主要包括系统初始化 *Setup*、签名产生 *Sign* 和验证 *Verify* 等，具体流程如下：

- 系统初始化 *Setup*：系统全局参数有 p、q 和 g，其中 p 和 q 均为大素数，$g \in Z_p^*$ 且 $g^q = 1 \bmod p$。系统的局部参数为 x 和 y，其中 $x \in [1, p-2]$ 为用户私钥，$y = g^x \bmod p$ 为用户公钥。
- 签名产生 *Sign*：假设需要签名的消息为 m，用户首先随机选取整数 $k \in [0, p-1]$，计算 $r = g^k \bmod p$，然后计算签名 $e = H(r, m)$，$s = (xe + k) \bmod q$，其中 $H(\ )$ 为安全的哈希函数。计算完成后，将 (e, s) 作为消息 m 的签名发送给签名验证方。
- 验证 *Verify*：验证者在收到消息签名 (e, s) 后，首先计算 $r' = g^s y^{-e} \bmod p$，然后计算 $H(r', m)$，最后验证等式 $H(r', m) = e$ 是否成立，若成立则签名有效，否则无效。

为提出更加安全且实用的多重签名方案，基于 Schnorr 签名的各类多重签名方案陆续被提出。目前也存在使用 Schnorr 类签名技术解决区块链技术遇到瓶颈的案例，2018 年 3 月，区块链开发者们发布了针对 Schnorr 类多重签名研究论文《Simple Schnorr Multi-Signatures with Application to Bitcoin》，该论文介绍了如何将 Schnorr 类多重签名应用于比特币区块链。通过多重签名，将多个签名合为一个签名，这样不仅节省了区块

链的空间，还使得区块链能够处理更多的签名，增加安全性。但该方案后又被证明并非安全的，目前越来越多的研究者投入到多重签名方案的研究，希望提出更加安全且高效的多重签名方案应用于区块链。而数字签名作为保障区块链安全的基础，一直是密码学研究者的研究重点，同样是 SimpleChain 的工作重心。

4.2 标准简约

作为分布式应用的核心特点，区块链上的智能合约将由商业主体中心化控制的商业逻辑转型成为了社区化公共监督的分布式应用。然而区块链的不可篡改性则决定了链上任何的智能合约都是不可撤回的，一切智能合约代码层的纰漏与漏洞都会成为对合约本身，甚至于整个区块链网络的巨大威胁。以太坊智能合约的 The DAO 所引起的硬分叉智能算是典型案例之一。

对于大多数普通合约开发者来说，其核心诉求在于有一种简便、直观而安全的方式来通过分布式的方式去实现商业逻辑。因此，创新型的合约语言与编程语句对此类用户来说仍然太过复杂。为了满足这类开发者的需求，SimpleChain 的“简约”开发工具以其模块化的合约功能，提供了安全、简便的合约开发模式。通过既定的功能模块，开发者用户只需要定制化调整部分参数，即可完成合约的编写，而功能模块则覆盖了大部分主流 DApp 的应用需求。

为确保模块的可用性与鲁棒性，“简约”开发工具由基金会技术指导委员会管理，并且模块代码接受全开源社区的审计。仅通过审计门槛后的代码才会被加入成为“简约”功能模块。成为模块后的合约功能通过 GUI 的方式向普通开发者提供。开发者只需要通过拖拽与可视化的方式即可完成合约编写、发布与接口对接，从而大大降低了 DApp 的开发门槛。

4.3 深度开发环境

对于高级开发者来说，更为复杂的合约逻辑需要被落实。此外，对于主链底层代码的升级建议也需要在更为成熟的开发环境中进行提交。因此，SimpleChain 将一套深度开发环境封装入了节点客户端当中，任何用户可以通过下载节点客户端在本地节点中对代码进行测试。开发者甚至可以自建私有链网络，进行验证。完成验证后的代码能够推送至公网，并接受全网开发者审计。其中，通过技术指导委员会审计的，且具有完整功

能的智能合约代码片段将被打包成为“简约”中的功能模块，进一步提供给普通合约开发者调用。

4.4 易用性部署

根据节点类型采用不同的节点工具。对于轻量用户节点，会使用便捷、高效地移动端。而对于要求较高的验证节点，具有简洁的部署工具，从部署验证到模板选择再到绑定一键式服务，同时提供丰富的视频教程与部署文档，避免操作过程中出现问题。除此之外，SimpleChain 还拥有可视化节点管理系统与云部署服务，方便节点加入和对节点进行管理。

4.5 安全性支撑与迭代

4.5.1 底层算法周期性调整

SimpleChain 采用 PoW 机制，若出现恶意节点数量过多、算力过高，会导致主链不稳定的情况，容易造成类似以太坊区块链 2017 年发生的硬分叉事件。为保证主链安全，SimpleChain 底层采用开放式算力，并进行算法周期性调整，防止大规模的算力军备竞赛，由此有效地维护区块延长的最终确定性。

4.5.2 可控子链开放度

为确保子链的安全性，SimpleChain 可对子链开发度进行控制，支持授权管理。可采用基于 PKI 体系的 CA 证书管理体系（可支持第三方 CA），针对节点部署与 IDE/API 访问权限控制，可设置仅经过授权的节点才有权限加入到子链网络中或使用子链服务，即子链内部的扩展许可链化。

4.5.3 支持多密码算法

SimpleChain 采用多密码算法，为了适用于多行业和多应用，支持的密码算法包括国际密码算法和国密算法。

密码算法是用于加密、解密等操作的数学函数，目前密码算法包括公钥密码（非对

称密码）、消息摘要算法等，而一个密码系统的安全性重点在于密钥的保密性，并非在于算法的保密性，因此国际密码算法和国密算法大部分是公开的，便于使用者使用这些算法。SimpleChain 为满足不同场景需求，子链可支持不同类型的密码算法，例如国际密码算法中 RSA、AES、SHA256 以及国密算法中非对称密码算法 SM2、对称密码算法 SM4 和消息摘要算法 SM3 等。

4.5.4 安全算法更新与迭代

随着技术发展，量子计算机对目前密码学体系产生了巨大的影响。由于量子计算具有天然的并行性，而这种并行性使得在电子计算机环境下的一些困难问题，利用量子计算机可以简单解决。现有的公钥密码是基于计算复杂性，因此量子计算机的超强计算能力使得现有的公钥密码受到了威胁。

目前主要有 Shor 算法和 Grover 算法可用于密码破译，Shor 算法是针对整数分解的量子算法，Grover 算法是一种量子数据库搜索算法。因此，在量子计算环境下，现在广泛使用的 RSA、ECC 公钥密码、EIGamal 等均不再安全。

虽量子计算机能够攻击现有很多密码算法，但还有一些问题量子计算机并不擅长，通过这些问题构建的密码就能够抵抗量子计算的攻击，这些密码算法统称为抗量子计算密码，例如格密码等。

除量子计算机的威胁外，还需要考虑密码算法抵抗传统攻击。因此在 SimpleChain 在后续发展过程中，采用的密码算法也会更新相应的更新与迭代，根据发展和应用需求，调整使用最佳的密码算法。

4.6 主链有效工作量证明（EPoW）

SimpleChain 为确保主链的安全性与最终性，并提供公平开放的共识模式，将采取工作量证明机制的技术路线。并将目标设定于构建有效工作量证明。

所谓有效工作量证明（Effective Proof-of-Work）即利用区块链分布式激励特点，将有效算力输出作为分布式算力类型，并进行工作量验证。从而改变现有工作量证明中仅对运算哈希的现状。SimpleChain 将在共识算法中引入矩阵运算的算法验证，使得共识运算的算力除了作为工作量证明用于竞争主链记账权之外，也能够被作为人工智能当中，深层神经网络每一层所需的矩阵乘法运算算力。

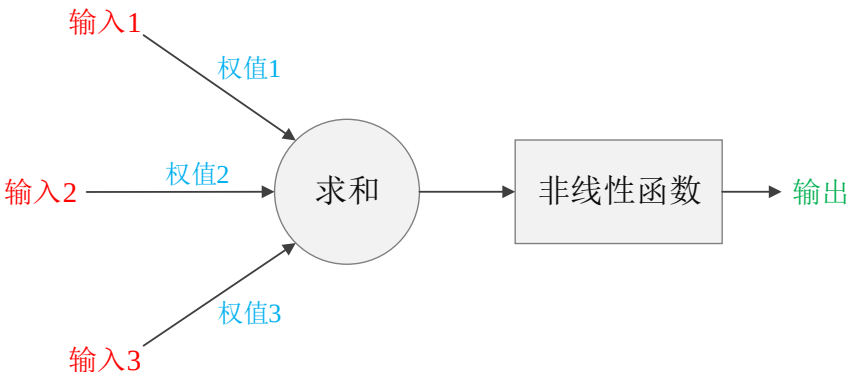

图 16 神经元模型

深层神经网络发展自人工神经网络，在人工神经网络中最基本的神经元结构是一个 MP 模型。如上图所示的典型神经元模型中，有三个输入，一个输出以及两个计算功能，而连接部分则是神经元模型中的重要组成部分，也就是权值。神经网络的训练算法的目的就在于通过调整权值，使得整个网络的预测效果能够调整到最佳[37]。

我们若将输入值分别以 a_1， a_2， a_3 表示，权值分别以 w_1， w_2， w_3 表示，则一个神经元模型用输出 b 公式表示如下：

$$b = f(a_1 \times w_1 + a_2 \times w_2 + a_3 \times w_3)$$

函数 $f(x)$ 包含了求和与非线性函数的表达。

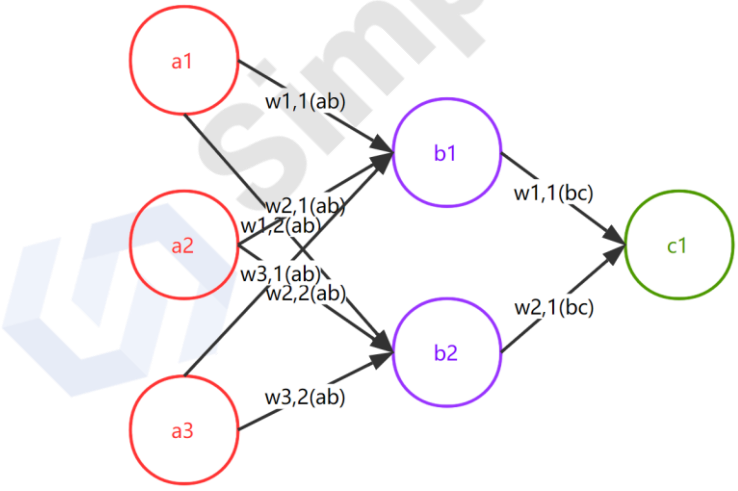

图 17 模型

当进入到深层神经网络中的感知器模型时，我们则在原本 MP 模型中的输入位置添加神经元节点，并标志为“输入单元”（红圈）。“输入单元”只负责传输数据，“输出单元”（紫圈）则需要对前一层的输入进行计算。

上图中的多层网络模型使用公式表示则为：

$$b_1 = f(a_1 \times w_{1,1}^{(ab)} + a_2 \times w_{2,1}^{(ab)} + a_3 \times w_{3,1}^{(ab)})$$

$$b_2 = f(a_1 \times w_{1,2}^{(ab)} + a_2 \times w_{2,2}^{(ab)} + a_3 \times w_{3,2}^{(ab)})$$

$$c_1 = f(b_1 \times w_{1,1}^{(bc)} + b_2 \times w_{2,1}^{(bc)})$$

通过以上推断，并进行抽象化则可表示为，每一层的大量计算是上一层的输出结果和其权重值这两个矩阵的乘法运算[38]。

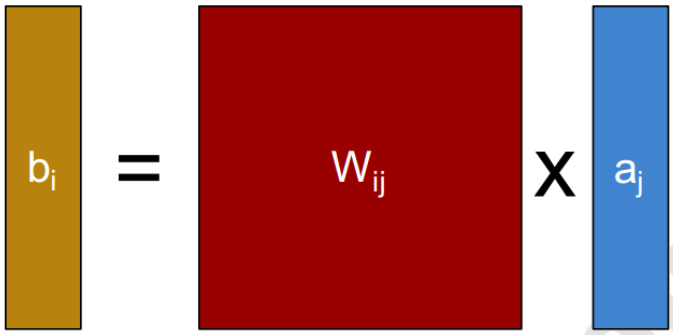

图 18 抽象化表达

而此类运算的逻辑与区块链当中前后区块头哈希之间形成的链状应用相似，因此通过在区块链共识算法中加入矩阵计算部分，能够使得工作量证明所消耗的算力至少在深度神经网络算法中被转化为有效工作量证明算力，服务于人工智能领域的运算。

比特币、以太坊等工作量证明区块链已实现了将分布式算力资产化，而有效工作量证明也将进一步实现有效分布式算力的资产化，并促进算力资源的流通与分配，提升资源利用效率，推动区块链当中所存在的中心化、安全、环保不可能三角问题的有效解决。

5 团队背景与组成

5.1 团队主要成员

高航

科技金融专家、财税信息化专家，资深技术极客，区块链领域早期创业者。曾任壹比特 CTO、浙金网 CEO、保全网 CEO，中国互联网协会国家互联网金融安全技术专家委员会委员，中国区块链应用研究中心常务理事。

俞学劢

浙江省区块链技术协会专家智库成员。英国金融风险管理理学硕士，拥有丰富金融机构工作经历。银行、证券、政务区块链应用项目负责人，算力宝联合创始人。曾于省级、国家级期刊发表多篇论文，并入选中国科协学术部区块链研究高产作者 Top 10。编著出版《区块链与新经济》、《区块链与人工智能》等书籍。

金

计算机专业硕士，密码学专家，具有多年区块链研究经验，长期从事区块链、大数据、人工智能等相关行业及技术研究，曾在国际学术会议和期刊发表学术论文，并申请了多项发明专利，参与编写出版了区块链书籍《区块链与人工智能》。

Moro Zhang

SimpleChain 技术负责人，资深技术专家，十余年游戏行业研发经验，曾担任保全网、杭州银行和兴业证券等项目的技术负责人，参与并负责多个行业联盟链构建及相关区块链应用开发。

覃昶栋

资深 dapp 开发工程师，具有多年应用开发经验，曾参与保全网、千信网、税易贷、算力网和算力国际站等多个项目的开发，目前在公链团队中主要负责研发 ChainBox、客户端等产品。

杨大敏

资深研发工程师，具有 8 年的游戏与支付研发经验，曾在多家公司担任软件研发工程师，在接触区块链并了解 SimpleChain 项目后，加入 SimpleChain 项目组参与区块链底层技术研发。

屈朋辉

SimpleChain 核心研发人员，资深研发工程师，同时掌握多种程序语言。曾担任 7 年 Java 软件工程师，参与了区块链在大数据、金融、存证等行业应用项目的研发，在 SimpleChain 团队参与研发链底层技术、智能合约等。

5.2 项目顾问

李侨峰

知名投资人，具有 20 年以上创投经验和投资管理经验，对私募股权投资领域和海内外资本市场有着独特深刻的见解和成功的投资经验。先后参与投资企业数十家，多家企业已成功上市。目前专注于 TMT、区块链、先进技术和智能硬件等领域投资。

Krzysztof Piech

拉扎尔斯基大学（波兰华沙）国际经济关系系教授和区块链技术中心主任，曾在华沙经济学院讲授约 20 年，Blockchain Technologies sp. z o.o.的首席执行官，波兰区块链技术加速器的领导者。Piech 教授还是国际分布式加密货币和区块链协会（莫斯科）的董事会成员，伦敦大学学院区块链技术研究中心的研究员，谢里夫理工大学伊朗区块链实验室的外部助理，编译出版超过 30 本书。

叶兆霖

新加坡丰汇能源集团董事局主席。三十年来，在新加坡主持了多个并购重组上市项目，具有资本市场的丰富经验。

6 上链基金会

6.1 基金会愿景与使命

SimpleChain 基金会是一个非盈利组织，是 SimpleChain 开源区块链社区的支持者和推动者。通过在全球范围内传播分布式新数字经济的理念，该基金会旨在形成一个活跃的开发者社区，这将有助于公共区块链基础设施的发展以及在此基础上的业务实施。它的使命是使 SimpleChain 成为一个全面值得信赖的生态系统，使得新的全球商业世界受益，同时降低成本，减少非对称性。

6.2 基金会组成

基金会常设机构由基金会理事会和基金会技术指导理事会两部分组成。基金会理事会负责整体管理 SimpleChain 社区的健康发展，基金会技术指导理事会则专注于 SimpleChain 技术本身的发展与技术社区的发展。两个常设机构分别以投票机制决策各自事务，基金会整体运营经费来自于 SimpleChain 社区的各类形式捐助。

6.2.1 基金会理事会

SimpleChain 理事会在基金会的早期阶段担任思想领导者，社区推动者和战略指导者。成员有义务投入包括知识，技能，资金和其他有形或无形资产在内的资源，使基金会充分运作。理事会的成员资格对 SimpleChain 开源社区的所有参与者开放。基金会理事会通过年度会议，进行业务决策，每 3 年完成一次理事会成员改选。

创始理事会由资深产业实践者，学术研究顾问与商业领袖组成。创始理事会理事成员数量为 7 人，并将在 1 年后通过链上选举机制扩张至 14 人。除了通过链上选举机制产生的主席拥有 2 票外，每一个理事会成员对于理事会决议拥有一票。

6.2.2 技术指导委员会

技术指导委员会是 SimpleChain 公共区块链基础设施技术开发的主管。在季度会议中通过技术指导委员会的多数批准，技术指导委员会可以做出决定，包括委员会成员的

资格和取消资格、接受 SimpleChain 基础设施编码版本控制和实施的升级建议、对新开发的模块或工具的确认或建议适用于开源社区的 SimpleChain 应用程序。该委员会的组成包括拥有丰富区块链经验的研究员、科学家和工程师，以及 SimpleChain 开源社区代码的优秀贡献者、SimpleChain 优秀智能合约与子链发布者。技术指导委员会的每个成员对季度委员会会议的任何技术提案都拥有 1 票的投票权。

创始技术指导委员会由 2 位拥有 3 年以上区块链经验的研究员、科学家或工程师组成，并各持有 1 票投票权。此外，基金会理事会整体对技术指导委员会决议拥有 1 票投票权。在基金会设立 2 年以后，技术委员会将增选至 7 名技术委员。除 2 名创始技术指导委员会委员外，将选举 SimpleChain 开源社区代码中被 merge 的前 2 名贡献者、SimpleChain 智能合约与子链前 3 名发布者作为增选委员。

6.3 基金会资金来源

基金会作为面向 SimpleChain 服务的非营利性组织，资金来源于 SimpleChain 社区参与者捐助的 SIPC。SimpleChain 基金会使用专属区块链地址与区块链智能合约账户进行募捐，募捐通过两个方式进行，直接募捐与算力募捐。

直接募捐，社区参与者通过基金会 SimpleChain 智能合约账户、以太坊智能合约账户、比特币地址、莱特币地址进行数字资产转账资助。

算力募捐，通过 SimpleChain 预设 PoW 规则，SimpleChain 全网算力产出 SIPC 奖励按 5%自动进入基金会 SimpleChain 智能合约账户，捐助比例每年减半。基金会智能合约账户根据预设规则将 10%的 SIPC 自动转至基金会理事会理事 SimpleChain 地址与技术委员会委员 SimpleChain 地址作为工资可自由提取，剩余 90%的 SIPC 及其他获捐数字资产作为基金会扩展、技术推广与其他运营使用，由理事会另行进行预决算。

此捐助规则意在对基金会理事、委员提供最低限度资金支持，并逐渐减少基金会在社区中控制力，同时减少单个节点对全网算力的垄断发生。

7 法律合规与风险控制

7.1 开源技术平台定义

区块链作为一项以多方参与为目的，分布式结构为特点，以及链上数据的公开、透明、可验证为原则的技术，从比特币将该技术提出以来就遵循开源软件思路，并坚持社区化运作为主流的发展路线。

作为公有区块链技术的 SimpleChain，为尽可能促进社区化开发力量的加入，并推动基于 SimpleChain 的应用子链网络的形成，开源区块链技术平台是其定位。主网上线后的 SimpleChain 将会全面对其初期团队所贡献的核心代码与工具代码进行全面开源，以支持社区开发者对上链的持续开发参与。

当然，开源并不代表无限制、无规则地免费使用或任意更改，开源技术需要秉承开放共享的精神的同时，根据各类开源许可证要求，进行规范性的使用。目前，已形成上百种不同类型的开源许可证，也各自有不同的要求。上链 SimpleChain 为促进广泛且深度的开发者社区的形成，从开源规则上将限制对源码修改后的闭源，并要求开发者新增的代码也同样遵循此规则，能够保持开发者社区扩展的持续性与连贯性。基于以上考虑，结合上链 SimpleChain 发起团队在 Linux 开源社区中的经验，上链 SimpleChain 的核心代码及工具组件代码将采用 GNU General Public License（GNU 通用公共许可证）即 GNU GPL。

GNU GPL[39]由自由软件基金会提出，提供 HTML、纯文本、ODF、Docbook v4\v5、Texinfo、LaTeX、Markdown、RTF 格式，用于嵌入其他文档当中使用。目前 GNU GPL v3 为最新版本，能够保护新开发者对于自身创作部分的版权，也同时进一步提供了拷贝、分发和修改的法律许可（Free Software Foundation, 2007）。上链 SimpleChain 将遵循此许可证约束并持续倡导社区维护 GNU GPL v3 的规则。

7.2 数字资产定义与备案要求

上链 SimpleChain 所设计的经济体系中，原生数字资产仅为 SIPC。SIPC 作为消耗性数字资产仅能够通过成为上链 SimpleChain 的验证节点，并运行 PoW 共识算法对区块链交易进行验证而获得。新区块的产生将根据算法对参与共识的验证节点进行 SIPC

奖励及验证手续费奖励，持有 SIPC 的节点可创建链上代码或子链，链上代码与子链的运行为获得其他验证节点的确认，需消耗 SIPC 支付验证费用，验证费用反馈到区块链网络用于激励验证节点，由此完成 SIPC 的供需循环。

根据当前美国 SEC、新加坡 MAS、瑞士 FINMA 等主流金融监管机构的论调，SIPC 作为消耗性数字资产或称 Utility Token，当前尚无备案申请要求。上链 SimpleChain 基金会作为发起者与开源社区管理者将确保项目符合业务当地法律法规，并根据新监管要求持续更新对上链 SimpleChain 社区的合规与风险控制的约束与建议。

7.3 社区治理与风险提示

上链 SimpleChain 是一项创新新区块链技术架构，SimpleChain Foundation 是上链 SimpleChain 区块链技术与区块链社区的发起方，承担早期技术的研发、社区的构建、与推广工作。作为非营利性组织，可接受适当捐助，用于维护上链社区健康发展，但不承担任何具体义务约束，不参与任何商业形式运作。上链 SimpleChain 社区中的子链及链上代码应用或有的商业价值与上链基金会无任何关联。

作为持续研发中的一项区块链技术与新兴建立的技术社区，可能由于上链 SimpleChain 开发的技术复杂性面临无法预测或克服的技术困难造成延期或特性削减，SimpleChain Foundation 将尽力发挥核心发起团队与社区力量推动技术迭代。代码可能由于存在瑕疵、错误、缺陷与漏洞造成安全性问题，通过开源公开，上链 SimpleChain 将接受社区验证，并接受任何形式的更新建议。

上链 SimpleChain 原生数字资产仅为区块链技术中的功能元素之一，并非任何类型实物、金融或货币资产，并与任何类型的实物、金融、货币资产无任何关联关系，SimpleChain Foundation 对其价值不做任何形式的保证。

附录：术语表

1、EPoW

Effective Proof-of-Work 简写，即有效工作量证明。利用区块链分布式激励的特点，将有效算力输出作为分布式算力类型，并进行工作量验证，改变目前工作量证明中仅进行哈希运算的现象。

2、通证

token 的中文翻译。

3、SIPC

SimpleCoin，即上链（英文名：SimpleChain）通证，可用于 SimpleChain 内部数据验证（交易）。

4、验证的交易容量与完成交易的实际时间

需主链验证交易时交易费用根据交易容量及完成时间决定，所谓交易容量为交易中数据的大小，而交易时间为 SimpleChain 区块链网络确定交易的时间。

5、多共识机制

多种共识机制，包括 PoW、PoS、PoC 等等，SimpleChain 为了满足和适应各类行业场景需求而设定。

6、节点

SimpleChain 区块链网络中节点包括主链普通验证节点、子链普通验证节点和跨链节点。

7、国际密码算法与国密算法

国际密码算法是由美国的安全局发布的密码算法，而国密算法由中国国家密码局认定的国产密码算法。

8、权限控制

为保证子链安全，对加入子链网络或者使用子链服务的节点进行开放度控制，只有授权的子链才能加入网络或者使用服务。

参考资料

[1] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System [Z]. bitcoin.org, 2008.

[2] Buterin, V. On Public and Private Blockchains [Z]. Ethererum Blog, 2015-08-07.

[3] Prusty, N. Building Blockchain Projects [M]. *Berminghan: Packt Publishing*, 2017.

[4] Digiconomist. Bitcoin Mining is more Polluting than Gold Mining [Z]. Digiconomist.net, 2018-01-16.

[5] Bentov, I. & A.Gabizon & A.Mizrahi. Cryptocurrencies without Proof of Work [J]. *Computer Science*, 2014:142-157.

[6] Snider, M. & K.Samani & T.Jain. Delegated Proof of Stake: Features & Tradeoffs [Z]. Multicoin Capital, 2018-03-02.

[7] Lamport, L. & R.Shostak & M.Pease. The Byzantine Generals Problem [J]. *ACM Transactions on Programming Languages and Systems*, 1982, 4 (3): 382–401.

[8] Castro, M. & B.Liskov. Practical Byzantine Fault Tolerance and Proactive Recovery [J]. *ACM Transactions on Computer Systems (Association for Computing Machinery)*, 2002, 20 (4): 398–461.

[9] Buterin, V. Long-Range Attacks: The Serious Problem With Adaptive Proof of Work [Z]. Ethererum Blog, 2014-05-15.

[10] 邵奇峰, 金澈清, 张召, 钱卫宁, 周傲英. 区块链技术：架构及进展[J]. 计算机学报, 2017:1-20.

[11] 姚前. 分布式账本技术研究进展综述[J], 武汉金融, 2018, (3):5-9.

[12] BTC.com. Network Status. btc.com, 2018.

[13] Top 500. TOP500 List – June 2018. www.top500.org, 2018.

[14] BitMEX Research. 比特币共识分叉的完整历史[Z]. blog.bitmex, 2018.

[15] 长铗. 不可能三角：安全，环保，去中心化[Z]. 8btc.com, 2014-02-04.

[16] 长铗. 计算即权力[Z]. 区块之链智能之芯, 2018-04-28.

[17] Bianews. 独家深度：BES 内部报告「FCoin 模式」详解[Z]. baijiahao.baidu, 2018.

[18] Odaily 星球日报. EOS RAM 价格暴涨会带来哪些负面影响？[Z]. 36kr.com, 2018.

[19] 中华人民共和国第十二届全国人民代表大会. 民法总则. 2017 年 3 月 15 日,第 127 条.

[20] 潘建萍，钱塘江畔崛起“中国区块链创新城市”：互联网法院成功维权，每日商报。

[21] 维基百科.“货币”词条. https://zh.wikipedia.org/wiki/%E8%B2%A8%E5%B9%A3#cite_note-3.

[22] William Stanley Jevons. Money and the Mechanism of Exchange, 1875.

[23] 维基百科.“金权政治”词条. https://zh.wikipedia.org/wiki/%E9%87%91%E6%AC%8A%E6%94%BF%E6%B2%BB

[24] 任碧云, 姚莉. 货币金融学. 北京: 中国财政经济出版社, 2009.

[25] The exploration of the path of super-sovereign currency. ResearchGate, 2017.

[26] 刘卫平. 美国货币政策调整及其影响研究[M]. 北京: 清华大学出版社, 2017: 51-54.

[27] 苗龙文. 现代货币数量论与中国“高货币化”成因[J]. 数量经济技术经济研究, 2007(12): 109-110.

[28] 曹家和. 宏观经济学[M]. 北京: 清华大学出版社,北京交通大学出版社, 2006:158-162.

[29] 万解秋, 徐涛. 货币供给的内生性与货币政策的效率[J], 经济研究, 2001(3): 41-42.

[30] Topic: Scalability and transaction rate [Z]. bitcointalk.org, 2010.

[31] Topic: dasg [Z]. https://bitcointalk.org/index.php?topic=125.msg1149#msg1149.

[32] Why mining variance matters? [Z]. https://medium.com/@lmgoodman/why-mining-variance-matters-80ef0ff4b183.

[33] 数字签名, 百度百科. https://baike.baidu.com/item/%E6%95%B0%E5%AD%97%E7%AD%BE%E5%90%8D/212550?fr=aladdin.

[34] K. Itakura and K. Nakamura. A public-key cryptosystem suitable for digital multisignatures [J]. *NEC Research and Development*, 1983, 71:1–8.

[35] Mihir Bellare and Gregory Neven. Multi-Signatures in the Plain Public Key Model and a General Forking Lemma [J]. In Ari Juels, Rebecca N.Wright, and Sabrina De Capitani di Vimercati, editors, *ACM Conference on Computer and Communications Security - CCS* 2006, pages 390–399.ACM, 2006.

[36] Claus-Peter Schnorr. Efficient Signature Generation by Smart Cards. *J.Cryptology*, 1991, 4(3):161–174.

[37] 史忠植. 神经网络[M]，高等教育出版社, 2009.

[38] 王玉伟. 深入理解 CPU 和异构计算芯片 GPU/FPGA/ASIC （上篇）[Z]. 云加社区, 2017.

[39] Free Software Foundation. GNU General Public License, 2007.