Katecoin

打造去中心化支付系统的信任基石

白皮书

前 言

自 2008 年金融危机爆发后，全球经济发生了巨大变革，以美国为代表的西方国家开始对已经运行近两百年的资本社会进行深刻反思。正在此时，密码学家中本聪发布了比特币白皮书《一种点对点的电子现金系统》。创新性的将加密密码学和分布式系统结合，解决拜占庭将军问题，促使比特币及背后区块链技术的诞生。由此虚拟货币开始走进大众视野，成为投资市场的新贵。随后在 2013 年 Vitalik Buterin 发布的以太坊初版白皮书，整个业界开始从加密货币时代进入区块链数字资产时代。

区块链技术被誉为未来十年内最有可能提高人类社会生产力的创新科技之一，其思想最早来源于比特币开源项目。它在发展过程中，借鉴了来自数字货币、密码学、博弈论、分布式系统、控制论等多个领域的技术成果，并依托分布式网络无需任何管理机构，通过算法和密码学原理来确保交易的成功进行。随着区块链技术和数资市场的持续发展和热度的持续升温，它给世界带来了无限的遐想空间和发展机遇，全球许多主要经济体已从国家战略层面开始对区块链技术及未来的趋势进行研究。

KateCoin 作为一种可以全球通用的数字货币，将致力于打造一个去中心化支付系统的信任基石，让其作为成功连接线上与线下、虚拟和实体经济的桥梁纽带，为提升生态效率和促进市场繁荣贡献一份力量。

目 录

摘　要

技术永远是推进行业发展的第一动力！

本白皮书将提出在基于 BTC（英文名：BitCoin，中文名：比特币，简称：BTC）的公有链生态体系下，采用 POW 共识机制来开发一种去中心化的数字加密货币，即 KTC（英文名：KateCoin，中文名：凯特币，简称：KTC)。KateCoin 选择用比特币作为技术底层，采用 POW 共识机制来执行货币的分配，算力越高、挖矿时间越长，获得的奖励就越多。Kate Coin 将致力于打造一个去中心化支付系统的信任基石，打通区块链与线下实体经济的结合，通过分布式思想促进虚拟经济及实体经济的融合及发展。KateCoin 团队非常认可比特币公链操作系统的开源开放精神，KateCoin 作为着重于服务于线下实体经济的桥梁纽带，会基于比特币开源系统做更多的业务层面上的改进，并促进自身社区与比特币社区的共同发展，KateCoin 的茁壮发展和比特币是紧密链接在一起的。

针对对应的生态体系，所有符合标准的实体资产都可在 KateCoin 生态中数字化并享受生态所带来的红利。

第 1 章. 背景概述

1.1 行业现状

自中本聪在 2009 年挖出了第一个比特币区块，到 2017 年 6 月，整个数字货币价值已上升至 2000 亿美元。整个数字货币市场的活跃，虽然有投机的属性存在，但根本的原因在与数字货币在流通、支付中的便利、灵活性以及对于全球资产去中心化标的预期。如今，加密数字货币作为一种新的技术和互联网金融业态，在全球范围里已引起了巨大反响，将对全球金融体系带来深刻地变革。中本聪提出区块链概念并创造比特币（BTC），开启了区块链世界的大门。

2015 年以太坊（ETH）横空出世，基于智能合约的区块链应用将区块链生态的演化再次向前推进。随着区块链技术的不断更新，各国政府及企业均注意到了区块链在价值传递、信息传输等领域存在的巨大潜力及价值。日本、澳大利亚等国家相继确立比特币（BTC）的合法地位；微软、摩根大通等企业巨头成立 EEA（企业以太坊联盟），开展基于以太坊的技术研究。区块链行业正在从初始的爆发当中走向成熟，其资产的兑换需求将呈爆发式的增长。

1.2 全球情况

从长远看，数字经济全球化是一个不可阻挡的趋势：

- ✓ 数字资产的灵活、便利，会取代一部分美元、黄金的作用。
- ✓ 可以显著降低支付、结算成本，从而在银行结算、跨国流通上

获得巨大的应用。

- ✓ 全球资产会数字化，未来的支付、投资、转账，都可以通过数字代币进行。
- ✓ 最终会有主权国家发起数字货币体系，这些国家的主权货币会和数字货币挂钩。

从国际层面看，越来越多的国家支持数字货币的发展：

- ■ 新加坡央行公布数字货币研究结果，基于以太坊私链的结算平台，“将代币化新加坡元（SGD，简称新币）搬到了分布式账本”平台中管理。
- ■ 自日本新规生效以来，比特币已成为一种合法的支付方式。日本央行金融技术主管更是宣称：区块链的发展应由私营企业领导， 央行不应阻止比特币创新。
- ■ 俄罗斯央行公开国家级数字货币研究计划。
- ■ 此外，据英国金融时报报导，全球最大的 6 家银行加入一个项目，拟启用一种新型数字货币，用于在区块链(blockchain)上清算和结算金融交易。
- ■ 巴克莱(Barclays)、瑞信(Credit Suisse)、加拿大帝国商业银行(CIBC)、汇丰(HSBC)、三菱日联金融集团(MUFG)和道富(State Street)已联手进一步研发“多功能结算币”(utility settlement coin)，这种货币由瑞士的瑞银(UBS)创建，希望能透过此一新型态的数字货币来提升金融市场效率。

1.3 未来趋势

区块链将对现有的经济社会产生巨大的影响，有望重塑人类互联网活动形态，对于区块链未来的发展将会呈现以下趋势。

- **多中心化**

  未来区块链系统架构将是构建可信任的多中心体系，将分散独立的各自单中心，提升为多方参与的统一多中心，从而提高信任传递效率，降低交易成本。即在信息不对称、不确定的环境下，建立满足各种活动赖以发生、发展的“信任”生态体系。

- **应用模式升级**

  鉴于公有链的安全性及交易量与日俱增对现网容量之间的平衡问题，比特币模式增加了区块链网络的维护成本，对于低价值、低风险的交易来说并非完全适用。未来区块链的应用领域将以联盟链、私有链或混合链为主。考虑到效率及安全的提升，未来将是以联盟链、私有链、或由联盟链和私有链组成的混合链组成。

- **智能合约社会化**

  未来，所有的契约型的约定都实现智能化，利用智能合约可以保障所有约定的可靠执行，避免篡改、抵赖和违约。除了将社会中的有形资产转变为数字智能资产进行确权、授权和实时监控外，区块链还可应用于社会中的无形资产管理，如知识产权保护、域名管理、积分管理等领域。

第 2 章. KateCoin 生态

2.1 产品诞生

综上所述，我们可以看出区块链已为全球社会区块链提供了一种新型的信任机制，为数字经济的发展奠定了新基石。且随着数字货币对传统市场项目的进一步冲击，再次证明数字货币及区块链技术对传统制度的颠覆性。而且这种颠覆正在不断加速，基于这样的时代背景与未来趋势，顺应着分布式思想的浪潮，一个真正能够链接数字经济领域及实体经济领域的 KateCoin 孕育而生。

相比于传统中心化数字货币，其优势在于：它有着去中心化、点对点传输、不可篡改、信息安全、面向全球范围等特点；其流通环节可以不依赖于任何中心化的发行系统，资产流通由单中心控制变成社会化传播，任何渠道资源都可以成为资产流通的催化剂。通过这种去中介化可以真正的实现利益的共享。因此，能极大地提升数据资产流通效率，真正达到自由流通的效果。

2.2 愿景目标

价值的创造者共享价值、真正回归本质。一切收益回归创造者，打破中心化的统治，真正做到去中心化。运用社区模式和 POW 工作量证明机制鼓励用户自发地组织、设计、交流，达成共识，共同构建 KateCoin 的未来。

第 3 章. 技术方案

KateCoin 作为一个可以全球通用的新型数字货币，基于 BTC 主网开创性地使用了 POW 算法，解决了安全性、高性能以及信任问题；从而在一定程度上极大的方便了资产的交易和流通。

3.1 技术原理

1）非对称加密技术

在传统加密和对称算法中，加密密钥能从解密密钥中推算出来，同时解密密钥也可以从加密密钥中推算出来。由此加密密钥和解密密钥是相同的，如果泄漏密钥就意味着任何人都可以对他们发送或接收的消息解密，所以这对于用户来说是极不安全的。

因此 KateCoin 在设计中使用了非对称加密技术，它和对称加密技术最大的不同就是有了公钥和私钥之分。非对称加密算法需要两个密钥：公开密钥(publickey)和私有密钥(privatekey)。公开密钥与私有密钥是一对，如果用公开密钥对数据和数字资产进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。在加密过程中使用公钥，在解密过程中使用私钥。公钥是可以向全网公开的，而私钥需要用户自己保存。由于不涉及私钥的传输，整个传输过程将变得安全很多。从而解决了对称加密中密钥需要分享所带来的安全隐患；这项技术将对应到 KateCoin 场景中的地址和私钥。

2）点对点传输技术

传统的数据储存、交易等方式都是建立在中心化机构之上，如果中心化机构遭到控制、或攻击，将会会损害到用户的利益，因此KateCoin 技术在开发时，运用了点对点传输技术，在无需中心化服务器的情况下、个体之间可以相互传输信息的技术。这将突破了传统中央服务器的瓶颈，具有无限的扩展性、稳定性和安全性，且任意节点都可以自由的加入或退出，越多节点参与，全网的性能将变得更高。从而实现了真正的去中心化。

3）哈希现金算法机制

为了保证系统的正常运行和防止作恶行为发生，KateCoin 使用了哈希现金(HashCash)算法机制，当用户产生交易时，就必须付出一定的工作量(proof of Work),并且在完成交易时盖上一个时间戳表示交易完成的时间。其主要目的是保证一笔数字货币没有被多次消费(Double Spending),这样就能保证发送方不能重复使用一个运算结果。每当用户贡献算力进行哈希运算时，作为回报 KateCoin 网络就会将一定数量 Token 赠予首个挖出区块的矿工作为回报。

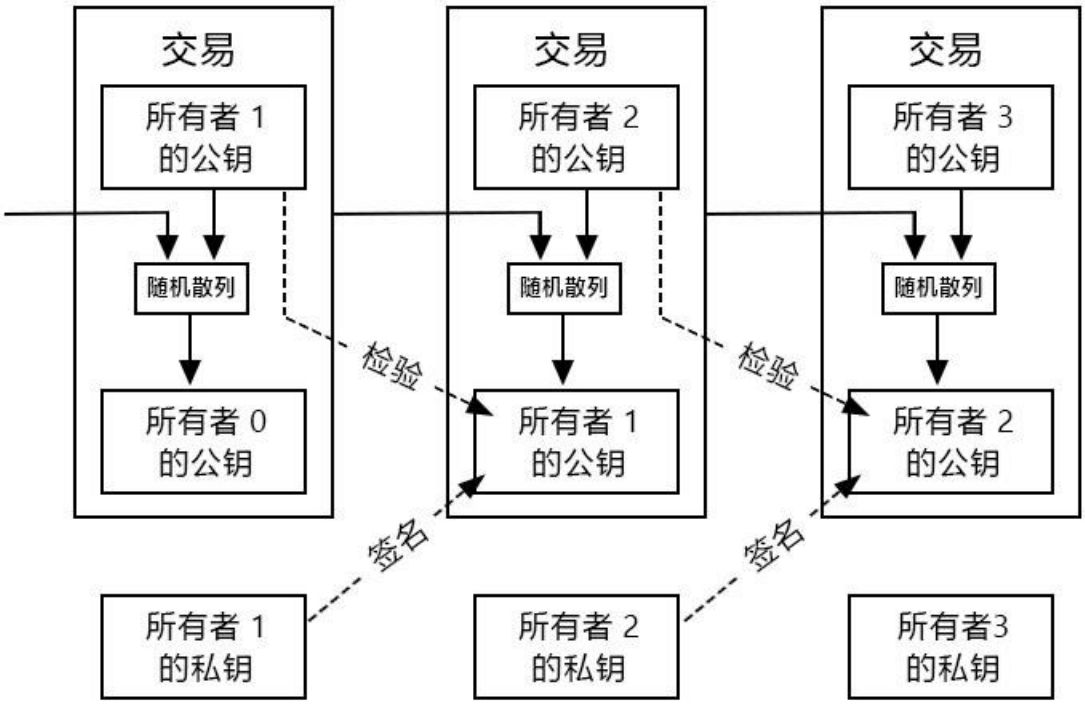
3.2 技术细节

为避免双重支付及双花问题的出现，KateCoin 通过随机散列（hashing）对全部交易加上时间戳（timestamps），并通过哈希对其加密，然后将其并入一个不断增长的哈希记录所组成的链条文件中，以此形成一个新的交易记录，这个哈希记录链条文件（以下简称

链条文件) 是由一个需要证明工作量的系统网路所提供存储和计算服务的。只要诚实的节点所控制的计算能力的总和，大于有合作关系的(cooperating)攻击者的计算能力的总和，那么 KateCoin 就是安全的。其具体实现原理和技术细节如下：

1)交易

我们将 KateCoin 定义成一串数字签名：每一位所有者通过对前一次交易和下一位拥有者的公钥(Public key) 签署一个随机散列的数字签名，并将这个签名附加在这枚 Coin 的末尾，Coin 就发送给了下一位所有者。而收款人通过对签名进行检验，就能够验证该链条的所有者。

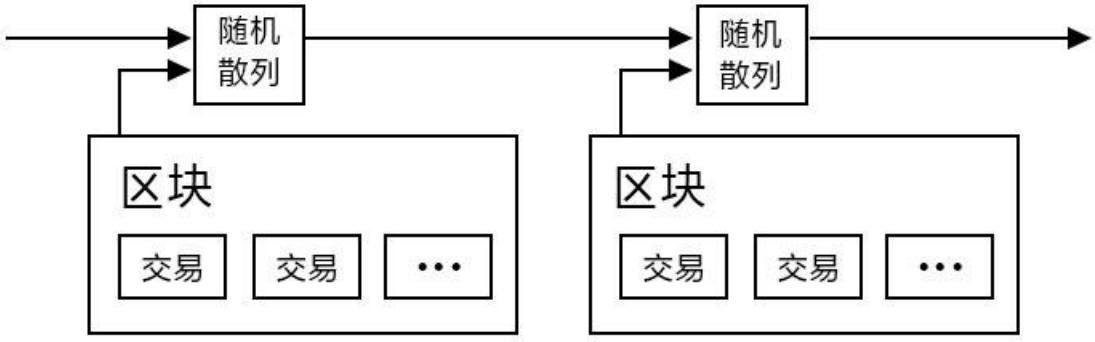


如果用户想要在 KateCoin 系统检测是否有第三方中介机构参与，那么交易信息就会被公开宣布，而在 KateCoin 系统中所有的参与者都

有唯一公认的历史交易序列。收款人只需要确保在交易期间绝大多数的节点都认同该交易是首次出现即可。

2）时间戳服务器

本解决方案首先提出一个“时间戳服务器”。时间戳服务器通过对以区块(block)形式存在的一组数据实施随机散列而加上时间戳，并将该随机散列进行广播，就像在新闻或世界性新闻组网络的发帖一样[2][3][4][5] 。显然，该时间戳能够证实特定数据必然于某特定时间是的确存在的，因为只有在该时刻存在了才能获取相应的随机散列值。每个时间戳应当将前一个时间戳纳入其随机散列值中，每一个随后的时间戳都对之前的一个时间戳进行增强(reinforcing)，这样就形成了一个链条（Chain）。



3）POST 算法

在比特币系统中采用了 PoW(工作量证明）算法,PoW 其实就是由所有的节点相互竞争，提交一个难于计算但是容易验证的计算结果，任何节点都可以验证这个这个结果的正确性，验证通过即算这个节点完成了大量的计算工作。

然而 PoW 机制存在明显的弊端。 一是算力不公平，矿场的竞争

力比单个节点大，还有就是随着硬件的发展，特别是量子计算机的出现，可能几秒就破解了 Hash。 二是 PoW 算法太浪费了，比特币网络每秒可完成数百万亿次 SHA256 计算， 但这些计算除了使恶意攻击者不能轻易地伪装成几百万个节点和打垮比特币网络，并没有更多实际或科学价值。有鉴于此， 人们提出了一些工作量证明的替代者。权益证明（ Proof of Stake， PoS）就是其中的一种方法。

权益证明（ Proof of Stake，PoS） ，最早在 2013 年被提出，最早在 Peercoin 系统中被实现，类似现实生活中的股东机制，拥有股份越多的人越容易获取记账权（ 同时越倾向于维护网络的正常工作） 。

典型的过程是通过保证金（ 代币、资产、名声等具备价值属性的物品即可） 来对赌一个合法的块成为新的区块，收益为抵押资本的利息和交易服务费。提供证明的保证金（ 例如通过转账货币记录）越多，则获得记账权的概率就越大。合法记账者可以获得收益。

PoS 试图解决在 PoW 中大量资源被浪费的缺点，受到了广泛关注。恶意参与者将存在保证金被罚没的风险，即损失经济利益。一般的，对于 PoS 来说，需要掌握超过全网 1/3 的资源，才有可能左右最终的结果。这个也很容易理解，三个人投票，前两人分别支持一方，这时候，第三方的投票将决定最终结果。

以现有的比特币运行发展情况来看， 比特币每年的挖矿产量都在不断减半， 我们可以预计， 随着比特币产量的不断降低， 矿工人数也会越来越少， 这样就会导致整个比特币网络的稳定性出现问题。

PoS 的解决方案是鼓励大家都去打开钱包客户端程序， 因为只有这样才可以发现 PoS 区块， 才会获得利息， 这也增加了网络的健壮性。还有当矿工数量变少的时候，比特币被 51%算力攻击就越容易。

4）网络

运行该网络的步骤如下：

a) 新的交易向全网进行广播；

b) 每一个节点都将收到的交易信息纳入一个区块中；

c) 每个节点都尝试在自己的区块中找到一个具有足够难度的工作量证明；

d) 当一个节点找到了一个工作量证明，它就向全网进行广播；

e) 当且仅当包含在该区块中的所有交易都是有效的且之前未存在过的，其他节点才认同该区块的有效性；

f) 其他节点表示他们接受该区块，而表示接受的方法，则是在跟 随该区块的末尾，制造新的区块以延长该链条，而将被接受区块的随机散列值视为先于新区快的随机散列值。节点始终都将最长的链条视为正确的链条，并持续工作和延长它。如果有两个节点同时广播不同版本的新区块，那么其他节点在接收到该区块的时间上将存在先后差别。当此情形，他们将在率先收到的区块基础上进行工作，但也会保留另外一个链条，以防后者变成最长的链条。该僵局（tie）的打破要等到下一个工作量证明被发现，而其中的一条链条被证实为是较长的一条，那么在另一条分支链条上工作的节点将转换阵营，开始在较长的链条上工作。 所谓“新的交易要广播”，实际上不需要抵达全

部的节点。只要交易信息能够抵达足够多的节点，那么他们将很快被整合进一个区块中。而区块的广播对被丢弃的信息是具有容错能力的。如果一个节点没有收到某特定区块，那么该节点将会发现自己缺失了某个区块，也就可以提出自己下载该区块的请求。

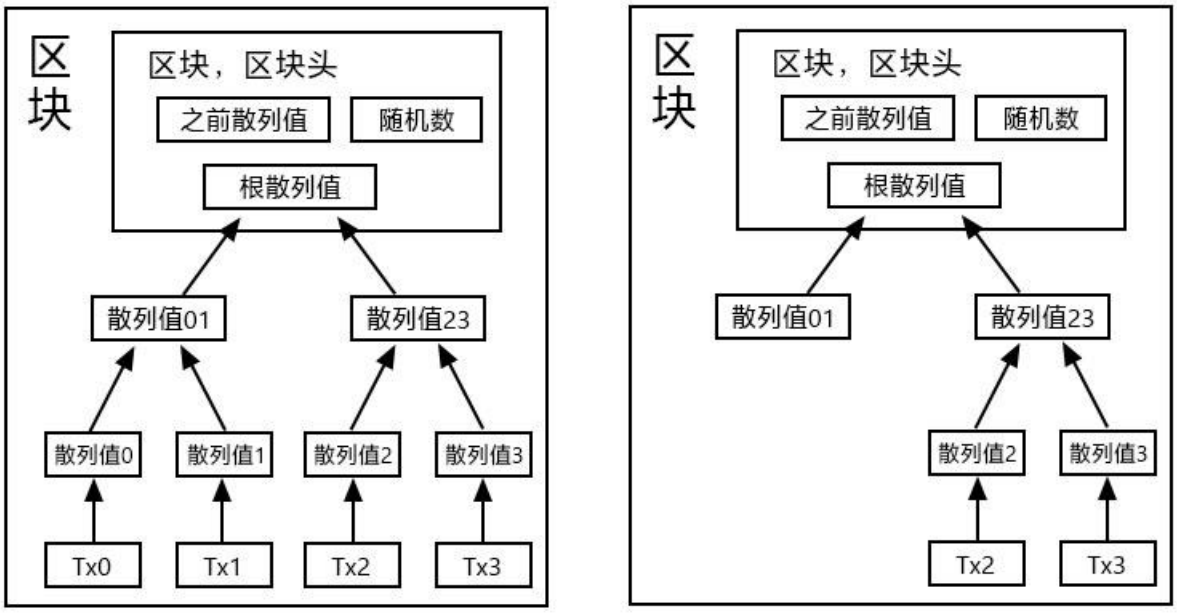
5)激励

当每个区块的第一笔交易进行特殊化处理，该交易产生一枚由该区块创造者拥有的新的 Coin。这样就增加了节点支持该网络的激励，并在没有中央集权机构发行货币的情况下，提供了一种将 Coin 分配到流通领域的一种方法。此时,另外一个激励的来源则是交易费（transaction fees）。如果某笔交易的输出值小于输入值，那么差额就是交易费，该交易费将被增加到该区块的激励中。只要既定数量的 Coin 已经进入流通，那么激励机制就可以逐渐转换为完全依靠交易费，在一定程度上 KateCoin 系统就能够免于通货膨胀的同时还有助于鼓励节点保持诚实。如果有一个贪婪的攻击者能够调集比所有诚实节点加起来还要多的 CPU 计算力，那么他就面临一个选择：要么将其用于诚实工作产生新的 Coin，或者将其用于进行二次支付攻击。那么他就会发现，按照规则行事、诚实工作是更有利可图的。因为该等规则使得他能够拥有更多的 Coin，而不是破坏这个系统使得其自身财富的有效性受损。

6）回收硬盘空间

如果最近的交易已经被纳入了足够多的区块之中，那么就可以丢弃该交易之前的数据，以回收硬盘空间。为了同时确保不损害区块的

随机散列值，交易信息被随机散列时，被构建成一种 Merkle 树（Merkle tree）的形态，使得只有根(root)被纳入了区块的随机散列值。通过将该树（tree）的分支拔除（stubbing）的方法，老区块就能被压缩，而内部的随机散列值就不必保存。



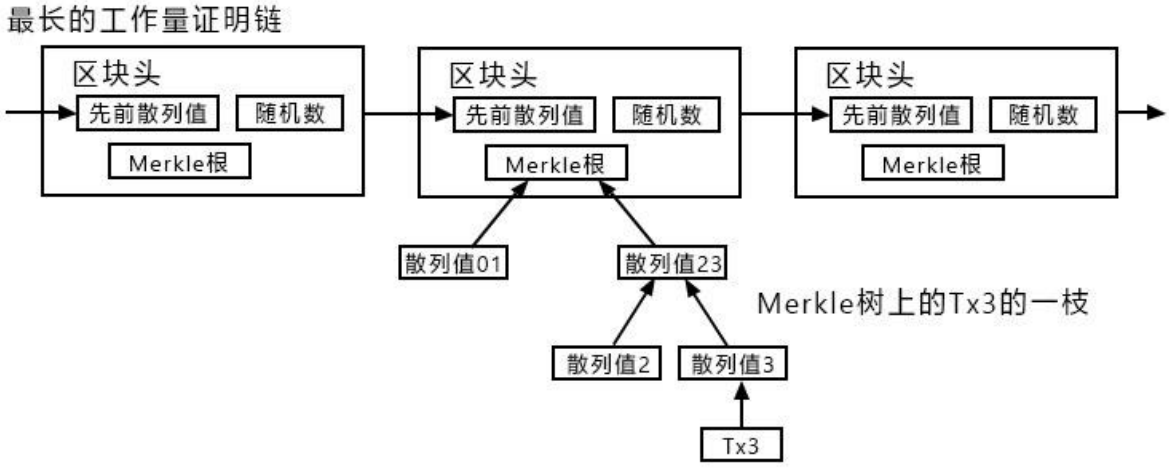
以Merkle树形式散列的交易　　将Tx0-2从区块中移除

不含交易信息的区块头（Block header）大小仅有 80 字节。如果我们设定区块生成的速率为每 10 分钟一个，那么每一年产生的数据位 4.2MB；（80 bytes * 6 * 24 * 365 = 4.2MB）。2008 年，PC 系统通常的内存容量为 2GB，即使将全部的区块头存储于内存之中都不是问题。

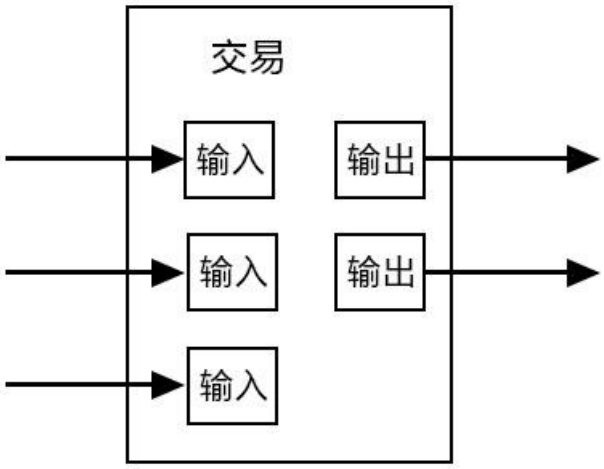
7）简化支付确认

在不运行完整网络节点的情况下，也能够对支付进行检验。一个用户需要保留最长的工作量证明链条的区块头的拷贝，它可以不断向网络发起询问，直到它确信自己拥有最长的链条，并能够通过 merkle

的分支通向它被加上时间戳并纳入区块的那次交易。节点想要自行检验该交易的有效性原本是不可能的，但通过追溯到链条的某个位置，它就能看到某个节点曾经接受过它，并且于其后追加的区块也进一步证明全网曾经接受了它。



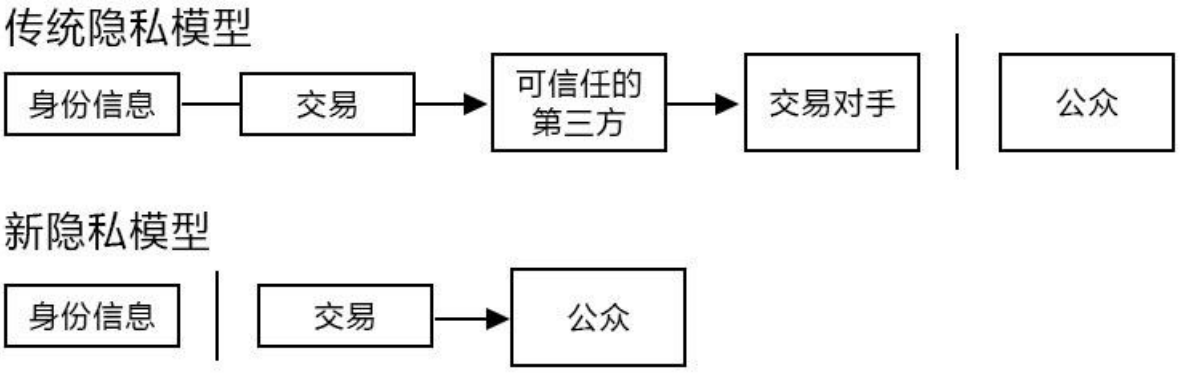
当此情形，只要诚实的节点控制了网络，检验机制就是可靠的。但是，当全网被一个计算力占优的攻击者攻击时，将变得较为脆弱。因为网络节点能够自行确认交易的有效性，只要攻击者能够持续地保持计算力优势，简化的机制会被攻击者焊接的（fabricated）交易欺骗。那么一个可行的策略就是，只要他们发现了一个无效的区块，就立刻发出警报，收到警报的用户将立刻开始下载被警告有问题的区块或交易的完整信息，以便对信息的不一致进行判定。对于日常会发生大量收付的商业机构，可能仍会希望运行他们自己的完整节点，以保持较大的独立完全性和检验的快速性。



8）价值的组合与分割

虽然可以单个单个地对 Coin 进行处理，但是对于每一枚 Coin 单独发起一次交易将是一种笨拙的办法。为了使得价值易于组合与分割，交易被设计为可以纳入多个输入和输出。一般而言是某次价值较大的前次交易构成的单一输入，或者由某几个价值较小的前次交易共同构成的并行输入，但是输出最多只有两个：一个用于支付，另一个用于找零。需要指出的是，当一笔交易依赖于之前的多笔交易时，这些交易又各自依赖于多笔交易，但这并不存在任何问题。因为这个工作机制并不需要展开检验之前发生的所有交易历史。

9）隐私



传统模型为交易的参与者提供了一定程度的隐私保护，因为试图向可信任的第三方索取交易信息是严格受限的。但是如果将交易信息向全网进行广播，就意味着这样的方法失效了。但是隐私依然可以得到保护：将公钥保持为匿名。公众得知的信息仅仅是有某个人将一定数量的货币发所给了另外一个人，但是难以将该交易同特定的人联系在一起，也就是说，公众难以确信，这些人究竟是谁。作为额外的预防措施，使用者可以让每次交易都生成一个新的地址，以确保这些交易不被追溯到一个共同的所有者。但是由于并行输入的存在，一定程度上的追溯还是不可避免的，因为并行输入表明这些货币都属于同一个所有者。此时的风险在于，如果某个人的某一个公钥被确认属于他，那么就可以追溯出此人的其它很多交易。

10）计算

当一个攻击者试图比诚实节点产生链条更快地制造替代性区块链。即便它达到了这一目的，但是整个系统也并非就此完全受制于攻击者的独断意志了，比方说凭空创造价值，或者掠夺本不属于攻击者的货币。这是因为节点将不会接受无效的交易，而诚实的节点永远不会接受一个包含了无效信息的区块。一个攻击者能做的，最多是更改他自己的交易信息，并试图拿回他刚刚付给别人的钱。 诚实链条和攻击者链条之间的竞赛，可以用二叉树随机漫步（Binomial Random Walk)来描述。成功事件定义为诚实链条延长了一个区块，使其领先性+1，而失败事件则是攻击者的链条被延长了一个区块，使得差距-1。攻击者成功填补某一既定差距的可能性，可以近似地看做赌徒破

产问题（Gambler’ s Ruin problem）。假定一个赌徒拥有无限的透支信用，然后开始进行潜在次数为无穷的赌博，试图填补上自己的亏空。那么我们可以计算他填补上亏空的概率，也就是该攻击者赶上诚实链条，如下图所示：

P = 诚实节点制造出下一个节点的概率

q = 攻击者点制造出下一个节点的概率

q_z = 攻击者最终消弭了z个区块的落后差距

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ \left(\frac{q}{p}\right)^z & \text{if } p > q \end{cases}$$

假定 p>q，那么攻击成功的概率就因为区块数的增长而呈现指数化下降。由于概率是攻击者的敌人，如果他不能幸运且快速地获得成功，那么他获得成功的机会随着时间的流逝就变得愈发渺茫。那么我们考虑一个收款人需要等待多长时间，才能足够确信付款人已经难以更改交易了。我们假设付款人是一个支付攻击者，希望让收款人在一段时间内相信他已经付过款了，然后立即将支付的款项重新支付给自己。虽然收款人届时会发现这一点，但为时已晚。 收款人生成了新的一对密钥组合，然后只预留一个较短的时间将公钥发送给付款人。这将可以防止以下情况：付款人预先准备好一个区块链然后持续地对此区块进行运算，直到运气让他的区块链超越了诚实链条，方才立即执行支付。当此情形，只要交易一旦发出，攻击者就开始秘密地准备一条包含了该交易替代版本的平行链条。 然后收款人将等待交

易出现在首个区块中，然后在等到 z 个区块链接其后。此时，他仍然不能确切知道攻击者已经进展了多少个区块，但是假设诚实区块将耗费平均预期时间以产生一个区块，那么攻击者的潜在进展就是一个泊松分布，分布的期望值为：

$$\lambda = z\frac{q}{p}$$

当此情形，为了计算攻击者追赶上的概率，我们将攻击者取得进展区块数量的泊松分布的概率密度，乘以在该数量下攻击者依然能够追赶上的概率。

$$\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\begin{cases}(\frac{q}{p})^{(z-k)} & \text{if } k \le z\\ 1 & \text{if } k > z\end{cases}$$

化为如下形式，避免对无限数列求和：

$$1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\left(1-\left(\frac{q}{p}\right)^{(z-k)}\right)$$

写为如下 C 语言代码：

#include double AttackerSuccessProbability(double q, int z) { double p = 1.0 - q; double lambda = z * (q / p); double sum = 1.0; int i, k; for (k = 0; k <= z; k++) { double poisson = exp(-lambda); for (i = 1; i <= k; i++) poisson *= lambda / i; sum -= poisson * (1 - pow(q / p, z - k)); } return sum; } 对其进行

运算，我们可以得到如下的概率结果，发现概率对 z 值呈指数下降。

当 q=0.1 时 z=0 P=1.0000000 z=1 P=0.2045873 z=2 P=0.0509779 z=3 P=0.0131722 z=4 P=0.0034552 z=5 P=0.0009137 z=6 P=0.0002428 z=7 P=0.0000647 z=8 P=0.0000173 z=9 P=0.0000046 z=10 P=0.0000012

当 q=0.3 时 z=0 P=1.0000000 z=5 P=0.1773523 z=10 P=0.0416605 z=15 P=0.0101008 z=20 P=0.0024804 z=25 P=0.0006132 z=30 P=0.0001522 z=35 P=0.0000379 z=40 P=0.0000095 z=45 P=0.0000024 z=50 P=0.0000006

求解令 P<0.1%的 z 值:

为使 P<0.001，则 q=0.10 z=5 q=0.15 z=8 q=0.20 z=11 q=0.25 z=15 q=0.30 z=24 q=0.35 z=41 q=0.40 z=89 q=0.45 z=340

11）结论

综上所述，通常的电子签名原理，是不足以防止双重支付。因此，KateCoin 在设计时提出了一种采用工作量证明机制的点对点网络来记录交易的公开信息，只要诚实的节点能够控制绝大多数的 CPU 计算能力，就能使得攻击者事实上难以改变交易记录。KateCoin 网络的强健之处在于它结构上的简洁性。节点之间的工作大部分是彼此独立的，只需要很少的协同。每个节点都不需要明确自己的身份，由于交易信息的流动路径并无任何要求，所以只需要尽其最大努力传播即可。节点可以随时离开网络，而想重新加入网络也非常容易，只需要补充接收离开期间的工作量证明链条即可。节点通过自己的 CPU

计算力进行投票，表决对有效区块的确认和不断延长有效的区块链来确认，也可在无效区块后延长区块以示拒绝。上述技术细节包含了 KateCoin 系统所需要的全部规则和激励措施。

3.3 技术特征

- **去中心化**

  通过 KateCoin 进行的每一次登记、确认、管理及交易等所有信息数据和凭证文件，均将分布式存储在区块链中，以实现永久性存储且不可篡改。

- **隐私保护**

  KateCoin 通过多重签名和不对称加密技术等方式提高系统中所有信息的安全性，未经授权的第三方没有能力访问系统内隐私信息。同时，参与者以匿名方式进行交易，第三方不能在未授权的前提下获取这些信息。通过非对称加密技术在区块链上存储数据可以达到一种完美的平衡，不会对区块链属性造成任何重大的改变。也就是说，区块链仍旧是公有区块链，但区块链上的数据将会被加密，因此照顾到了公有区块链的隐私问题，非对称加密技术使公有区块链具有私有区块链的隐私效果。

- **高安全性**

  由于涉及到资产交易，KateCoin 对数据的安全性、合规性要求非常严格，这得益于团队多年的金融行业从业经验，对于安全体系进行了充分的设计、规划，辅助以区块链技术的非对称加密机

制、分布式数据记账、防篡改等特性，形成了业务管理规范结合技术解决方案、研发与交互分离等高数据安全性设计。

3.4 技术优势

- **高效**

  借助于 Bitcoin 底层区块链设施的对区块数据的并行处理优化，并通过 Bitcoin 的架构可支持秒级的确认时间和强大的事务处理吞吐率。

- **兼容**

  基于 Bitcoin 底层区块链的工作机制，KateCoin 可以面向整个生态圈提供数据服务，实现链内链外数据转移和互通。

- **参与**

  用户可以通过节点参与全球范围内的共识体系和生态运转。独特的治理策略可以促使节点遵守社区规则，并利用 Bitcoin 特有的算法保证 KateCoin 系统的正常运行。

第 4 章. 关于凯特币

4.1 KateCoin 简介

【中 文 名】 凯特币

【英 文 名】 KateCoin

【简　　称】 KTC

【算　　法】 SCRYPT

【发行总量】 4200 万枚

【发行时间】 2013 年 11 月

【LOGO 标识】

KateCoin —— 是一种虚拟的可以全球通用的 P2P 形式的数字货币，与大多数货币不同，它依据特定算法通过大量的计算产生，且不依靠特定的货币机构发行。该币总数量非常有限，具有一定的稀缺性。年产最多 100 万个，总量有 4200 万个，通过“挖矿方式”生成。根据其设计原理，凯特币的总量会持续增长，直至 40 多年后达到 4200 万的那天。但随着越来越多的人接受并使用凯特币，它的挖矿

难度会越来越大，同样的挖掘方式获取的凯特币将越来越少。在支持凯特币消费的商家里，持有者可以直接使用凯特币进行消费支付。在支持凯特币的交易平台里面，也可以自由的购买凯特币并持有，或出售凯特币获取流动法币。

4.2 产生原理

KateCoin 通过“挖矿”方式产生，“挖矿”是一个具有竞争力和去中心化的过程。这一过程包括个人为凯特币网络服务，并因此得到回报。凯特币的矿工使用专用的硬件处理交易和保护凯特币网络，并在交易时收集新的凯特币。

其协议的设计方式是以固定的速率发行新的凯特币，这使得凯特币的挖矿成为一个竞争极为激烈的行业。当越来越多的矿工加入凯特币网络，赚取利润变得越来越难。任何中央管理机构或开发者都无权控制或操纵该系统以提高他们的利润。任何行为如不符合该系统要求遵循的规则，都将被全世界任何一个凯特币节点所拒绝。凯特币以一个可预测的逐步下降的速率发行，新产生的凯特币数量会逐年减半，直到凯特币的总数达到 4200 万个。到那时凯特币矿工也许只能通过大量的小额交易费用来支持。

要挖掘凯特币可以下载专用的凯特币运算工具，然后去矿池网站注册，把注册来的用户名和密码填入计算程序中，再点击运算就正式开始。完成凯特币钱包客户端安装后，可以直接获得一个凯特币地址，当别人付钱的时候，只需要自己把地址贴给别人，就能通过同样的钱

包客户端进行付款。

第 5 章. 管理组织

KateCoin 社区将由设立在美国的基金会进行管理。该机构作为 KateCoin 社区的法律主体，将全权负责 KateCoin 的技术开发、业务推广、社区运营等工作，且承担所有 KateCoin 的法律责任。为了确保整个 KateCoin 社区在公开透明的状态下高效运行，将设立 KateCoin基金委员会(以下简称基金会),在KateCoin基金委员会下，设立决策委员会——基金会最高决策机构，管理基金会旗下各个执行机构，有权决定基金会资金使用、冻结、奖励、惩罚等，决策委员会成员由社区选举产生。决策委员会任期为 2 年，在任期满后，将由 KateCoin 社区选举产生。

其中决策委员会下设立 5 个执行机构，具体分布如下图所示：

业务委员会—— KateCoin 的业务推广、商业拓展、生态搭建等，成

员一般由子类目应用公司代表担任。

技术委员会—— KateCoin 技术开发管理、代码开源管理、Github 开源代码维护、社区技术更新评估等，成员一般由国内外区块链技术专家担任。

社区委员会——国内外社区运营和管理、国内外社区活动策划、国内外社区资源对接、社区奖励发放、社区惩罚执行。成员一般由社区活跃成员担任。

公共关系委员会—— KateCoin 项目进展通报、公关问题处理、对外宣传等，成员一般由 KateCoin 签约公关公司代表担任。

人事财务委员会——负责基金会成员的日常补贴发放、正常财务支出、志愿者招募等。

执行机构责任人——决策委员会成立后会任命各个执行机构的负责人，负责人将承担相关业务职能下的运营管理、个人机构间的工 作协调，负责人定期需向决策委员会汇报工作。

第 6 章. 团队介绍

6.1 创始团队

Arthur Yang，KateCoin 项目创始人，拥有十余年互联网行业发展及管理经验，熟悉主流区块链技术架构及原理，全栈工程师，连续创业者。曾负责多个区块链项目的设计、研发和运营，先后完成了基于区块链技术的数字资产、公示存证、实体投资、公益捐助、社会服务等多个项目论证与开发；具有丰富的区块链系统研发和管理经验。

Jerry An KateCoin 项目核开发人员。兼具前/后端软件项目开发经验，对前端 HTML，CSS，JS 有深厚的技术功底，擅长解决兼容性问题，深入掌握 jQuery，Bootstrap，react，Less，Sass 等技术框架。

Marcos Chow，KateCoin 联合创始人，7 年风险投资管理经验，曾为多家 A 股上市公司提供战略规划及商业模式设计、组织变革与升级、人才培养等服务。区块链资深爱好者，参与过多个区块链项目市场运营管理，对区块链社区运营管理有深入的了解。

6.2 天使投资人

近 30 位资深金融行业公司高管鼎力支持 KateCoin 项目，作为天使投资人给予了 KateCoin 项目资金、行业资源、业务发展等多方面的支持和帮助。他们是 KateCoin 长期快速发展的坚实后盾和有效助

力；天使投资人详细名单参见后续官网公布。

第 7 章. 发展路线

通过以上所述，我们相信 KateCoin 会推动区块链应用创新落地，真正打造一个新的安全、稳定、高效且可信的区块链支付一站式服务平台。为此我们开发团队作为狂热的互联网和区块链爱好者，将投入百分百热情和资源来实现我们的愿景和目标，与 KateCoin 用户一起颠覆传统中心化统治的平台。

KateCoin 项目开发计划一览表

步骤	时间	里程碑	工作内容
第一阶段	2013 年 05 月	项目立项，技术开发。	项目方案准备，项目计划书编写。开始进行区块链技术研发，构建软件环境开发。
第二阶段	2013 年 11 月	1.0 版本开发完成，上线。	推出首个版本，按内测、公测流程上线并做市场推广，增加用户。
第三阶段	2014 年 02 月	优化原有版本，上交易平台。	此版本将透明更多细节数据，增强用户体验。
第四阶段	2015 年 06 月	布局产业链，拓展应用。	高精度定位用户需求，拓展渠道，增加更多运用场景，提升用户粘性。
第五阶段	2016 年 12 月	技术突破	建立完善的推广奖励机制及透明的入驻机制，完善生态系统增加代币价值。
第六阶段	后续	颠覆	不断更新，持续升级。

第 8 章. 风险提示

用户应慎重考虑下列风险并用清晰的判断能力去评估项目、自身财务状况及风险承受能力而作出投资决策，并承担由此产生的全部损失。

1）系统风险

KateCoin 团队将不遗余力实现白皮书中所描述的发展目标，尽管创始团队在区块链行业已经积累了十分丰富的人脉资源与经验，但项目的拓展依然存在不可预见的潜在难度，从而使得项目可能面临进展不如预期的风险。在市场方面，如未来数字资产市场的整体情况发生变化，将加大本次投资的风险。另一方面，系统性风险还包括一系列不可抗力因素，包括但不限于自然灾害、计算机网络在全球范围内的大规模故障、政治动荡等。

2）政策风险

我们认为，全球各国可能在不久的未来陆续出台规范区块和电子代币的相关监管政策与法规。未来政策存在一定不确定性，随着政府有关众筹项目的政策发生重大变化或是相关的政策、法规出台，将引起众筹市场的波动,代币的发行、价格均会受到影响从而给众筹参与者带来风险。此外，KateCoin 所涉及的公司数资交易也可能在未来

面临着政府的监管加强的风险。

3）团队风险

KateCoin 团队由在资本市场和互联网及区块链领域具有丰富经验的人士组成，吸引到了区块链领域的资深从业者、具有丰富经验的技术开发人员等。但在今后的发展中，依然存在着核心人员离开、团队内部发生冲突而导致项目整体受到负面影响的可能性。

4）技术风险

目前区块链技术仍处于探索和发展阶段，区块链行业面临着人才缺乏、人才竞争激烈的现状，区块链、分布式账本、去中心化、不可篡改等技术支撑着核心业务发展，KateCoin 团队不能完全保证技术的落地；同时，项目在发展过程中，不排除由于技术测试及技术路线预估不充分，从而给项目开发进度带来一定影响，导致项目中断或终止。

5）代币风险

代币的使用范围与用户和市场的认可度直接相关，在项目完成测试并上线使用后，最终代币在链上及实体场景的接受度和普及度存在不确定性，从而影响持有者的代币使用及交易，且项目方对此不承担回购或赎回义务。

第 9 章. 免责声明

一、本白皮书所传递之内容仅供参考，不构成 KateCoin 团队及其相关公司中出售股票或证券的任何投资买卖建议、教唆或邀约。此类邀约须通过机密备忘录的形式进行，且须符合相关的证券法律和其他法律。

二、本文档内容不得被解释为强迫参与 Token 公开发行。任何与本白皮书相关的行为均不得视为参与 Token 公开发行，包括要求获取本白皮书的副本或向他人分享本白皮书。

三、KateCoin 团队将不遗余力实现文档中所提及的目标，然而基于外界因素的存在，团队不能完全做出完成承诺。

四、KateCoin 团队将不断进行合理尝试，确保本白皮书中的信息真实准确。开发过程中，平台可能会进行更新，包括但不限于平台机制、代币及其机制、代币分配情况。文档的部分内容可能随着项目的进展在新版白皮书中进行相应调整，团队将通过在网站上发布公告或新版白皮书等方式，将更新内容公布于众。请参与者务必及时获取最新版白皮书，并根据更新内容及时调整自己的决策。

五、拥有 KateCoin 不代表授予其拥有者对平台的所有权、控制

权及决策权。 KateCoin 作为在数字资产中使用的加密代币。均不属于以下类别任何种类的货币:

(a) 证券;

(b) 法律实体的股权;

(c) 股票、债券、票据、认股权证、证书或其他授与任何权利的文书。

六、KateCoin 的增值与否取决于市场规律的应用情况，也可能受到市场参与者的影响。团队不对其增值做出承诺，并对其因价值增减所造成的后果概不负责。

七、KateCoin 团队将遵守任何有利于行业健康发展的监管条例以及行业自律申明等。参与者参与即代表将完全接受并遵守此类检查。同时，参与者披露用以完成此类检查的所有信息必须完整准确。

八、参与者披露用以完成此类检查的所有信息必须完整准确。KateCoin 团队明确向参与者传达了可能的风险。参与者一旦参与互换，代表其已确认理解并认可细则中的各项条款说明，接受本平台的潜在风险，后果自担。