CartyCoin白皮书V2.0

2019.10.10

摘要

CartyCoin简称 CC。总量 8800 万，流通总量800万。采用莱特 SCRYPT 共识算法，全部通过挖矿产生，没有任何预挖和所谓的团队创世独占，后期每天产币4032CC，币少珍稀，值得关注！。

CC委员会
CartyCoin@outlook.com

第1章　项目背景和意义

自2009年比特币诞生以来，区块链技术得到了长足的发展。以比特币为代表的数字加密货币逐渐被人们所了解和接受，成为去中心化的数字资产和价值存储。比特币被人们称为数字黄金。2013年，天才少年VitalikButerin和技术极客GavinWood创建的以太坊项目也获得了巨大的成功。越来越多的基于以太坊智能合约的去中心化应用广受人们关注。而这一切都是基于区块链技术的推动。

根据coinmarkcap.com统计数据，全世界目前有超过4000种数字加密货币。全部市场价值合计超过6000多亿美元，并且仍然处在高速增长中。数字加密货币的基石，区块链技术，也必将影响到每一个人类的衣食住行，并对人类社会的当前以及未来的所有行业产生冲击。

然而在一片喧嚣之中，区块链世界却不是一片祥和，实则危机四伏。

1.1 可扩展性问题

BTC网络当前一笔交易手续费平均达到0.001BTC以上，折合￥100以上，高峰期是这个值的4倍，这使得BTC用于普通支付不再可能，与初衷背道而驰，曾经落地的应用不但没能流行，反而慢慢关闭，游戏平台Steam就因此叫停比特币支付，甚至于1月18日在迈阿密市中心举行的北美比特币大会(TNABC)，也取消比特币付款购买门票。这种关闭支付通道的趋势将继续蔓延，目前并无解决方案。

区块链很有前景，但在不久的将来，会出现区块链作为一个支付平台，其本身不能覆盖全球的电子商务的情况。区块链是一个点对点协议，把原来国家银行担当的结算机关由所有的参与者代替。比特币网络中的每个节点必须了解在全球范围发生的每一个交易，这可能造成对涵盖全球的网络造成阻碍。相反，若能涵盖全球所有金融交易，并且不会损失安全性，才是最佳解决方案。

支付网络Visa在2013假期期间，在其网络上每秒实现47000交易（TPS），目前实现平均每天数亿笔交易。而比特币因为1兆字节块的限制，每秒仅支持小于7笔交易。如果每次比特币交易我们平均用300字节，并假设块大小无限制，达到与Visa峰值47000/TPS

的交易量同等数据容量意味着每十分钟每比特币区块将近8千兆字节数据。持续下去，每年的数据将超过400万亿字节。显然，如今在比特币网络上获得Visa般的能力是不可行的。在世界上没有家用电脑可以有那样的带宽和存储。如果比特币在未来替换所有的电子支付，而不仅仅是Visa，这将导致比特币网络的彻底崩溃，或者在最好的情况下，只有可以支付得起的比特币节点和矿工可以使用。这种集中化会再次打败网络分散化，使比特币安全受到威胁。

为了实现用比特币进行每秒多于47000笔交易，需要脱离比特币区块链本身进行交易。如果比特币网络支持以极低的费用每秒进行近乎无限数量的小额交易会更好。许多小额支付可以按顺序在两方之间发送，使任何大小的付款成为可能。小额支付将使服务变得非捆束，少信任，商品化。如支付每兆字节的互联网服务。为了能够实现这些小额用例，将需要大幅降低最终被公布的链上交易的数量。

1.2 应用落地问题

另一方面，伴随着BTC价格一路高涨，虚拟币世界成员日渐增多，每天都有多种新型的投入市场，然而实际落地能产生效益，服务社会的极少。将聚焦于提升支付能力，解决网络拥堵，并开发出重量级应用，发挥出区块链技术的优势。

第2章CC的架构与技术方案

2.1 点对点通信

点对点价值传输网络的出现有其历史必然性，而Satoshi则是加速这个历史进程的人。从上个世纪80年代，TCP/IP协议的开发，到90年代，网页浏览器的应用和服务器的应用，一直到今天，互联网技术从不同侧面和维度改变了数据交换的模式和人类的生活。互联网技术的发展得益于基础设施的完善，从早期的信息高速公路（InformationSuperHighway）和各种智能终端的普及，这些也构成了互联网OSI七层模型中，应用层无限拓展的基础。在互联网的各种协议栈中，我们用的较多有TCP/IP，HTTP，HTTPS，FTP，TELNET，SSH，SMTP，POP3等网络层，传输层，应用层的协议，并且借助这些协议，我们已经比较完美了搭建了各种各样的互联网服务。但是如果我们深思，我们会发现，在比特币网络出现之前，我们一直无法互联网上面，在不借助于第三方的情况下，较好的进行点对

点的价值的转移和传输。其实我们并不是缺少一种特定的方法，而是缺少基于信息高速公路（InformationSuperHighway）的价值高速公路（ValueSuperHighway），以及如何实现ValueSuperHighway的ValueTransferProtocol（VTP协议），而比特币网络则是运行于信息高速公路上面的第一个VTP协议。

P2P具有分散化(Decentralization)、扩展性、健壮性、隐私性、高性能等特点。P2P网络通信的效率对区块链整体性能的影响非常重要，尤其是影响了整个区块链网络的速度。针对物联网中各接入CC 的物联网设备和用户，从会话维护、地址确定、通信机制、存储方案等方面进行了深度的优化。通过指定用户端与共识节点的关联物理配置和规模数量，并采分片处理(sharding)机制和高速网络连接，从而减轻共识节点的通信、计算和存储负担，改善区块链的交易性能,从而达到针对物联网设备区块化的最大性能，为以后物联网设备的登记、数字化、认证和安全提供基础保证。

2.2 CC 数字签名加密算法

信息的加解密是区块链的关键环节，主要是哈希函数和非对称加密两部分的算法。

1）哈希函数部分，目前主要有SHA、MD5等多种算法，还包括算法的串联和并联使用。由于商业应用一般更注重性能问题，所以CC 基础算法以SCRYPT算法为主。

2）非对称加密部分，主要有非对称加密算法包括RSA、DSA、椭圆曲线算法等，区块链一般使用椭圆曲线算法，包括ECDSA和SCHNORR，考虑到Schnorr签名的验证速度比ECDSA签名更快，而且这种签名体积可以更小，还原生地支持多重签名。而这也正符合物联网小体积的特性，所以CC 基于Schnorr开发了自有的SDSchnorr算法。

同时，CC 模块化的设计，可替换多种加密算法。由于物联网用户接入的帐户和形式多样，安全性要求并不一致，所以CC 也集合了国密算法(SM2椭圆曲线公钥密码算法、SM3密码杂凑算法、SM4分组密码算法)。同时，CC 对底层加密算法库进行了抽象以及算法的可替换通道，以满足不同物联网应用的算法及安全需求。

2.3 CC 共识算法

CC 在Block的生成过程中使用了POW机制，一个符合要求的BlockHash由N个前导零构成，零的个数取决于网络的难度值。要得到合理的BlockHash需要经过大量尝试计算，

计算时间取决于机器的哈希运算速度。当某个节点提供出一个合理的BlockHash值，说明该节点确实经过了大量的尝试计算，当然，并不能得出计算次数的绝对值，因为寻找合理hash是一个概率事件。当节点拥有占全网n%的算力时，该节点即有n/100的概率找到BlockHash。

2.4 CC 智能合约

CC 在继承区块链技术既有优势的同事，将逐步支持智能合约。智能合约犹如操作系统一般，可以使得各种应用能在链上开发。**2.4.1**智能合约的概念形成智能合约是被称为“区块链2.0”的代表性产物，但其理念很早就被提出来了，可追溯到1994年，几乎与互联网同期出现。

给予这一概念名字“智能合约”的是密码学家尼克萨博，他因为比特币打下基础而受到广泛赞誉，萨博的关于智能合约如何工作的理论还没有实现，因为没有天生的能够支持可编程交易的数字金融系统，这在当时是一种极具前瞻性的理念。

而比特币的出现和广泛使用，正在改变阻碍智能合约实现的现状，从而萨博的理念有了重生的机会。

2.4.2 理解智能合约智能合约是一种可以自动化执行的简单交易。举一个简单的例子：我跟你打一个赌，如果明天下雨，算我赢，如果明天没下雨，就是你赢了。然后我们在打赌的时候就把钱放进一个智能合约控制的账户内，第二天过去了，结果出来了以后，智能合约就可以根据收到的指令自动判断输赢，并进行转账。这个过程是高效，透明的执行过程，不需要公正等第三方介入。也就是说，有了智能合约以后，就不能赖账啦。这只是个简单的例子方便大家理解，智能合约还有很多应用的地方可以在此基础上进行深度开发。

到底什么是智能合约呢？智能合约概念可以概括为:一段代码(智能合约),被部署在分享的、复制的账本上，它可以维持自己的状态，控制自己的资产和对接收到的外界信息或者资产进行回应。或者可以这样简单的概括：它是运行在可复制、共享的账本上的计算机程序，可以处理信息，接收、储存和发送价值。

智能合约程序不仅仅只是一个可以自动执行的计算机程序，它更像是一个系统的参与者，可以把它想象成一个绝对可信的人，他负责临时保管你的资产，并且严格按照事

先商定好的规则执行操作。

2.4.3 智能合约的工作原理基于区块链的智能合约包括事务处理和保存的机制，以及一个完备的状态机，用于接受和处理各种智能合约；并且事务的保存和状态处理都在区块链上完成。智能合约的触发需要满足时间描述信息中的触发条件，当条件满足以后，从智能合约自动发出预设的数据资源。智能合约系统的核心在于进入智能合约的是一组事务和事件，经过智能合约处理后，出来的也是一组事务和事件。它的存在只是为了让一组复杂的、带有触发条件的数字化承诺能够按照参与者的意志，正确执行。

2.4.4 智能合约的构建及执行步骤

基于区块链的智能合约的构建及执行分为如下步骤：

1、智能合约的构建：由区块链内的多个用户共同参与制定一份智能合约；

2、智能合约的存储：智能合约通过P2P网络扩散到每个节点，并存入区块链；

3、智能合约的执行：智能合约定期进行自动机状态检查，将满足条件的事务进行验证，达成共识后自动执行并通知用户。

2.4.5 智能合约的现状目前，智能合约系统主要有以太坊（Ethereum），以太坊是一个开源的区块链底层系统，就像安卓一样，提供了非常丰富的 API 和接口，让许多人在上面能够快速开发出各种区块链应用。目前已经有超过 400 多个应用在以太坊上开发。以太坊主要是使用 Solidity 编写智能合约，并在微软云服务上提供了智能合约工具箱，运行在以太坊区块链上，其平台因多功能性和智能合约执行能力成为银行业和互联网金融行业的首选，纳斯达克、摩根大通、VISA 和高盛等多家金融机构均使用以太坊的智能合约系统。

2.4.6 **CC** 的智能合约之路可以看到，智能合约拥有广泛的前景，拥有了智能合约，CC 对接应用将变得非常容易，而区别于以太坊的高手续费，高延时，CC 可以做到低费用高效率。

2.5 环签名方案

2001年，Rivest等人在如何匿名泄露秘密的背景下提出了一种新型签名技术，称为环签名（RingSigna-ture）。环签名可以被视为一种特殊的群签名（GroupSignature），由于群签名需要可信中心和安全的建立过程，往往在匿名保护上存在漏洞（签名者对于可信

中心是可追溯的），而环签名在群签名基础上去除了可信中心和安全建立过程，对于验证者来说，签名者是完全匿名的，所以环签名更具实用价值。

自环签名提出后，大量学者发现其重要的价值，基于椭圆曲线、门限等多种环签名方案被设计开发，总体概括可分为门限环签名、关联环签名、可撤销匿名性环签名、可否认环签名四类。

为实现区块链上智能合约代币交易隐私保护，我们使用一种基于椭圆曲线的环签名方案。环签名可分为三个部分：GEN，SIG，VER，以签名者账户公私钥对(P,x)为例说明三个过程：

GEN：采集公共参数，签名者利用GeneratePublicKeySet()函数在CC 账户系统中随机选取n-1个账户，与签名账户共同构成环签名公钥集publickeyset：

publickeyset=GeneratePublicKeySet(P)

签名者利用公私钥对(P,x)，通过GenerateKeyImage()函数生成公

钥镜像I：

I=GenerateKeyImage((P,x))

SIG:完成环签名。针对所需签名消息m，利用环签名公钥集

publickeyset,公钥镜像I和签名账户私钥x通过

GenerateRingSignature()函数生成环签名ringsig：

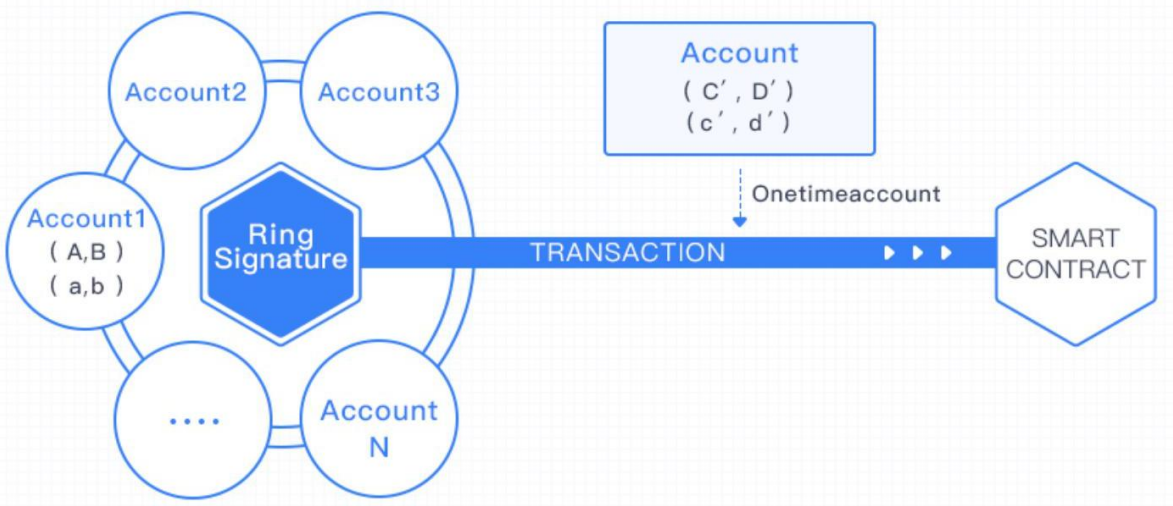
ringsig=GenerateRingSignature(m,publickeyset,I,x)

VER：验证环签名。基于消息m，利用环签名公钥集publickeyset，公钥镜像I和环签名ringsig，通过VerifyRingSignature()验证签名合法性：

flag=VerifyRingSignature(m,publickeyset,I,ringsig)

flg=true则签名合法；flg=false则签名不合法。

环签名设计方案中，由于环签名公钥集publickeyset中公钥账户真实存在，公钥镜像I和环签名ringsig均与签名账户无法对应，使得签名账户的匿名隐私性得以保证。交易验证者只能确定签名合法，且签名者是publickeyset中某一账户，却无法进行准确定位。



第3章CC 的应用规划

3.1 CC生态发展规划

3.1.1 去中心化的开源交易所传统交易所因其缺乏监管和不透明，成为一块法外灰色区域，其操纵行情，恶意爆仓，吃取撮合差价，制造假行情，甚至篡改交易记录，已广为人所诟病，究其根本，就是不透明，而开源交易所能解决这一切。

去中心化的开源交易所并不需要传统的服务器架构，因为其后端体系结构是部署在区块链上的智能合约。它一个分布式应用程序，当用户在交易所上进行“交易”时，他们必须创建一个可用于与此智能合约进行交互的钱包，或将现有的钱包连接到交易所以便与智能合约进行交互操作。也就是说，用户的一切交易，实际上都是发生在链上的真实事件，将被记录在区块数据中，无法作伪。

当前已经有人在ETH网络中尝试开源交易所，但因公有链的承载能力已到瓶颈，手续费高企和延时大，使得交易行为大受限制，几乎无法通过买卖获利，而私有链可以完美的解决这一问题。

去中心化的开源交易所将是CC 重点发展方向。

3.1.2 借贷

随着数字货币成为更加广泛的交易媒介及更加重要的价值储藏载体，利用数字货币创造新的价值并获得相应收益是必然趋势，正如将比特币投资于“挖矿”，投资于其他区块链项目ICO类似。随着数字货币应用范围的不断增加，利用数字货币直接(不需要转换为法币，投资的收益也以数字货币计价)进行投资的领域和机会逐渐增多。利用数字货币创造价值的人需要更多的数字货币，手中持有数字货币的人需要保值增值，数字货币

的借贷业务需求会越来越多。CC 支持具有信用和资金能力的机构或者个人作为数字货币的供需中介，完成存贷业务。以以太币举例，实现方式是中介方在CC 上利用智能合约创建存款应用并设定利息，以太币存入方通过跨链机制将以太坊上的以太币转入CC 上的智能合约对应的地址，CC 上的存款智能合约发放对应该笔存款的凭证（CC 上的token，类似银行的存单）到CC 上该用户的账户中，智能合约自动计算利息。当用户需要提取该笔以太坊存款时，将凭证转移回中介地址，合约执行跨链交易将凭证对应的以太币在原链上解锁转移回原有用户的账号中。该场景优于传统模式的重要一点总是，作为存贷中介方的存款准备金（该中介地址对应的被锁定的原链资产）是透明的，作为存款人能时刻知晓存款准备金情况。

3.1.3 数字货币支付结算

越来越多的商户正在接收比特币等数字资产作为支付手段，未来会有更多的商业场景将多种数字货币作为支付媒介。对于用户来说无论在电脑和手机上安装多个钱包进行支付都是不方便的，正如目前的支付需要VISA，Paypal，支付宝这样的中介机构进行支付结算的统一整合。

CC 本身是一个分布式的多币种平台。从本质上说正如第三方支付将不同银行的账本接入在自己的统一账本下一样，CC 实现数字货币领域的类似功能。任何商户和用户都可以安装CC 钱包完成多币种的支付结算功能，而不需要安装多个数字货币钱包。

3.1.4 数字货币交易兑换

目前完成数字货币的兑换主要依赖于中心化的交易所场外交易中间人。所有交易都基于对交易所和中间人的信任。多币接入 CC 后，交易所或者中间人可以通过智能合约实现多币种的竞价交易和一对一的场外交易。CC 上提供隐私保护的交易机制，为有隐私保护需求的交易提供支持。将没有隐私保护的数字货币导入 CC ，并在 CC 中发起隐私交易，最终再将数字货币转回原有链，一定程度上通过切断资

金追踪路径实现了原有链的隐私保护。这一使用场景类似于较早出现过的混币模式。

3.1.5 资产投融资

我们已经看到传统的资产以联盟链的形式映射到区块链上的趋势，例如商业票据、商业积分、未来收益权、应收账款等。未来会有更多的金融资产以基于联盟链的分布式账本形式记录。当这些联盟链接入 CC 后，联盟链成为金融资产的提供方，数字货币的持有者可以利用手中的数字货币购买这些资产进行投资。类比传统银行业务，这类似于在银行购买理财产品。区别在于更多的中介机构可以参与进来，或者资产持有人可以直接进行资产融资。ICO 现已成为区块链领域众筹融资的重要手段，且这一趋势正向非区块链领域蔓延。越来越多的项目，尤其是基于以太坊的项目，直接使用智能合约进行 ICO，整个过程更加透明公平，但是只能使用以太币进行众筹，给持有其他数字货币的投资者造成了不便。基于 CC 开发的 ICO 平台，或者单独的 ICO 项目，发行方以智能合约进行发行的同时，可以支持多币种进行投资。投资人能够更加方便的用以太坊、比特币或者其他任何与 CC 连接的区块链代币进行投资，发起方可以更加便利的管理自己募集的资金。

3.1.6 其他应用场景上面描述的是最基本的应用场景，目的在于让读者更好的理解 CC 的运行逻辑和价值。举一反三可以想到，通过 CC ，可以发行基于数字货币的多币种信用卡；可以将多种资产打包进行资产证券化操作；可以进行基于多种数字货币的 P2P 业务，众筹业务等。区块链技术在银行中的应用已经被各大银行视为重要战略，但出发点多是基于如何利用区块链技术改造传统业务；而数字货币领域货币兑换等类银行的业务已经在蓬勃发展。区块链在这两个领域的进展，如同两条平行线。随着数字资产在经济中的比重日益提升，与现实经济的融合不断增强。这两条平行线同样会走向融合：数字资产进入银行的资产负债表（银行支持数字资产的存贷），银行的资产负债表部分转移到区块链上（法币以区块链 token 的形式表示和记账）。CC 跨账本资产转移的特性将能够支持未来的融合。

3.2 CC 管理架构

CC 社区将由设立在新加坡的基金会进行管理。该机构作为 CC 社区的法律主体，将全权负责 CC 的技术开发、业务推广、社区运营，并且承担所有 CC 的法律责任。为了确保整个 CC 社区在公开透明的状态下高效运行，CC 将设立

CC基金委员会（以下简称基金会），在CC基金委员会下，设立有：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CC社区选举产生。

3.2.1 各部门职责

各部门负责的事务具体如下：

1）技术委员会：负责技术管理工作，具体工作包括开源代码管理，代码开发、代码修改、代码测试、代码审核、代码上线、漏洞修复、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。

2）应用委员会：负责 CC 上线后的应用场景落地工作，资产尽责调查、资产合规性审核、资产信息披露、资产交易管理等。

3）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。

4）财务及人事委员会：负责整个项目募集资金的使用和审核、开发人员薪酬管理、日常运营费用审核等。

5）法务及风控委员会：负责境内外公司的注册登记、审核各类协议，对法律事务给出专业意见，开展法律知识的培训，提高各部门人员的法律意识。

6）市场及公共关系委员会：市场及公共关系委员会目标是为社区服务，负责CC 推广、产品推广、开源项目的推广和宣传等。

7）执行机构责任人：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。此外，委员会还负责对外公告管理。

3.2.2 披露义务为保护投资人利益，加强原生数字资产的管理和高效使用，促进 CC 项目健康发展，设置信息披露制度。CC 发起团队承若将谨慎勤勉的原则管理和运用原生数字资产。希望通过自身示范作用，规范原生数字资产的管理，增加区块链行业的自律，提升区块链加密数字资产管理的透明度，维护好区块链行业的长远发展。定期信息披露，在每个会计年度之日起三个月内编制并披露年度报告，每个季度结束后的两个月内披露

季度报告。报告内容包括不限于 CC 的技术开发里程碑及进度、应用开发里程碑和进度，数字资产管理情况，团队履职情况，财务情况等。临时信息披露，CC 基金会

应及时报告项目的重大合作事项、核心团队成员变更、涉及到 CC 的诉讼等将在官网披露信息报告。

2 法务法律事务：CC 若出现需要寻找法律意见的事项，需要通过律师予以确认。免责条款：CC 为非赢利性组织，用户获取的是 CC 的使用权，购买者应明白在法律范围内，CC 不做任何明示或暗示的保证。

争议解决条款：当出现争议时，有关方面应依据协议通过协商解决。如协商无法解决，可通过法律解决。

3.2.4 财务资金来源：维持 CC 项目运作的资金来源于原生数字资产，在需要的时候部分原生数字资产会转换为法币，以拥有必要的支付资金。财务管理说明：基金会财务管理的原则：统筹安排，综合管理；勤俭节约，讲求实效；精打细算，量入为出。基金会资产管理纳入全民预算管理，根据实际运用情况，编织财务收支预算。年度财务收支预算报自制委员会审议，月度财务预算由执行委员会审议，财务及人事委员会负责编制和执行，将在官网披露每个季度的财务报告。

CC 基金会将引入第三方审计，监督项目的财务运作，进行资金审计和提供审计报告，审计报告将在年度信息披露中公告。

3.2.5 成员介绍

首届决策委员会成员由区块链、物联网领域知名行业专家组成，简要介绍如下：

1. CoreDavidPan 联席主席美国加洲大学柏克利分校本科、美国金门大学企业软件系统硕士、美国哈佛大学金融财经硕士。前Arm亚太区物联网市场总监，及美商亚晶国际资本总经理。具备20年北美及亚洲科技公司及风险投资管理经验，相关产业包括：物联网、半导体、软件、电子制造、电信产业。

2.周昕RichardZhou联席主席加拿大多伦多GreenPandaMarketingInc.总裁，并为多家世界500强及NaCCq上市公司担任顾问，加中天使联盟顾问，曾任多伦多证交所上市公司

InternetofThingsInc.(TSX.v-ITT）独立董事，多伦多国际电影节（TIFF）中国互联网影视发展论坛共同主席，曾任加拿大最大慈善机构之一的多伦多病童医院慈善基金华裔委员会的创会理事，加拿大常青会会长，曾任加拿大安大略省旅游文化体育厅厅长助理。周昕有着20年的计算机、互联网、物联网、能源互联网从业和创业经验，曾在加拿大EMC，西门子，Apotex等企业担任高级系统工程师。

核心技术团队成员：

1、CoreDavidPan执行负责人

美国加洲大学柏克利分校本科、美国金门大学企业软件系统硕士、美国哈佛大学金融财经硕士。前Arm亚太区物联网市场总监，及美商亚晶国际资本总经理。具备20年北美及亚洲科技公司及风险投资管理经验，相关产业包括：物联网、半导体、软件、电子制造、电信产业。

2、Fauda.Khan

国际标准组织(ISO/IECSC27)加拿大主席，IOT特殊工作组召集人；ISO/IECSC41的国际召集人；现任TwelveDotLabs的首席执行官及安全分析师，为全球客户提供网络安全解决方案；超过21年以上的网络安全行业经验。

3、高沃博士

北京邮电大学学士、英国伦敦玛丽女王大学硕士、博士。国际物联网专家、英国伦敦玛丽女王大学电子工程与计算机科学学院教授、IEEE资深会员，同时在科技金融领域有多个IPO项目经验。

4、许文玻硕士

上海复旦大学软件工程硕士，8年C++服务端软件开发、架构设计，4年研发团队管理经验。曾负责开发过上海电信"游戏新天地"平台、PCLBS精准位置服务、互联网用户画像及数据挖掘、苏州银行集中作业批量验印和各家银行电子验印项目等，并于近期主导完成了ARM公司mbedos的区块链模块包开发，拥有行业极少数的区块链物联网项目落地开发经验，和丰富的软件安全系统开发能力。

CC 顾问团队：

1、Hugo博士

瑞典皇家理工学院教授。前新加坡金管局执行总监。

2、EduardMolla

阿尔巴尼亚驻华经济参赞。

3、梁宾先

台湾物联网协会理事长，华苓科技股份有限公司董事长兼任总经理，南京邮电大学海峡两岸智慧服务产业研究院院长，中国工信部电子商会物联网技术产品应用专业委员会副会长，感知中国物联网商会/联盟执行会长，江苏省物联网技术与应用协同创新中心常务理事，浙江省汽车工业技术创新协会/副会长，无锡海峡两岸科技金融服务中心/副理事长，台湾云端物联网产业协会(CIAT)/技术专家委员会委员，台湾区电机电子工业同业公会云端巨资与物联网委员会委员。

3.3 CC 的审计相关

由于虚拟币在现有政策下的特殊性，CC 基金会无法被现有的制度监管，但为了保证整个 CC 的公开透明，CC 决策委员会将聘请专业的审计机构进行审计并且公开。

第4 章产品规划

2016年6月立项2016年7月团队核心成立2016年9月开发，科研成果验证2017年7月CC上线测试2018年2月挖矿试运行2018年2月第1个区块（创世块）成功挖出100个CC2018年2月全面开放钱包，挖矿2018年6月（预计）上线交易平台2018.12－协助合作伙伴接入，持续扩大。

第5 章免责申明

本文档只用于传达信息之用途，并不构成买卖项目股份或证券的相关意见。任何类似的提议或征价将在一个可信任的条款下并在可应用的证券法和其他相关法律允许下进行，以上信息或分析不构成投资决策或具体建议。

本文档不构成任何关于证券形式的投资建议，投资意向或教唆投资。本文档不组成也不理解为提供任何买卖行为，或任何邀请买卖、任何形式证券的行为，也不是任何形式上的合约或者承诺。本文档中所有的收益和利润举例仅为展示目的，或代表行业平均

值，并不构成对用户参与结果的保证。CC 明确表示相关意向用户明确了解 CC 平台的风险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意个人为此承担一切相应结果或后果。

CC明确表示不承担任何参与CC项目造成的直接或间接的损失包括:

(i)本文档提供所有信息的可靠性

(ii)由此产生的任何错误，疏忽或者不准确信息

(iii)或由此导致的任何行为。本文档以最终版本为准，本版本为测试版。

第6 章风险提示

数字资产投资作为一种新的投资模式，存在各种不同的风险，潜在投资者需谨慎评估投资风险及自身风险的承受能力：

1、虚拟币销售市场风险

由于虚拟币销售市场环境与整个数字货币市场形势密不可分，如市场行情整体低靡，或存在其他不可控因素的影响，则可能造成虚拟币本身即使具备良好的前景，但价格依然长期处于被低估的状态。

2、监管风险

由于区块链的发展尚处早期，包括我国在内全球都没有有关ICO过程中的前置要求、交易要求、信息披露要求、锁定要求等相关的法规文件。并且目前政策会如何实施尚不明朗，这些因素均可能对项目的投资与流动性产生不确定影响。而区块链技术已经成为世界上各个

主要国家的监管主要对象，如果监管主体插手或施加影响则CC应用可能受到其影响，例如法令限制使用、销售诸如CC有可能受到限制、阻碍甚至直接终止CC应用和CC的发展。

3、竞争风险随着信息技术和移动互联网的发展，以“比特币”为代表的数字资产逐渐兴起，各类去中心化的应用持续涌现，行业内竞争日趋激烈。但随着其他应用平台的层出不穷和不断扩张，社区将面临持续的运营压力和一定的市场竞争风险。

4、人员流失风险

CC集聚了一批在各自专业领域具有领先优势和丰富经验的技术团队和顾问专家，其中不乏长期从事区块链行业的专业人员以及有丰富互联网产品开发和运营经验的核心团队。核心团队的稳定和顾问资源对CC保持业内核心竞争力具有重要意义。核心人员或顾问团队的流失，可能会影响平台的稳定运营或对未来发展带来一定的不利影响。

5、资金匮乏导致无法开发的风险

由于创始团队筹集的CC价格大幅度下跌或者开发时间超出预计等原因，都有可能造成团队开发资金匮乏，并由此可能会导致团队极度缺乏资金，从而无法实现原定开发目标的风险。

6、私钥丢失风险

购买者的CC在提取到自己的数字钱包地址后，操作地址内所包含内容的唯一方式就是购买者相关密钥(即私钥或是钱包密码)。用户个人负责保护相关密钥，用于签署证明资产所有权的交易。用户理解并接受,如果他的私钥文件或密码分别丢失或被盗,则获得的与用户帐户(地址)或密码相关的CC将不可恢复,并将永久丢失。最好的安全储存登录凭证的方式是购买者将密钥分开到一个或数个地方安全储存，且最好不要储存在公用电脑。

7、黑客或盗窃的风险

黑客或其它组织或国家均有以任何方法试图打断CC应用或CC功能的可能性，包括但不限于拒绝服务攻击、Sybil攻击、游袭、恶意软件攻击或一致性攻击等。

8、未保险损失的风险

不像银行账户或其它金融机构的账户，存储在CC账户或相关区块链网络上通常没有保险保障，任何情况下的损失，将不会有任何公开的个体组织为你的损失承保。

9、核心协议相关的风险

CC平台目前基于比特币技术开发，因此任何以该技术导致的漏洞，不可预期的功能问题或遭受攻击都有可能导致CC或CC平台以难以预料的方式停止工作或功能缺失。

10 、系统性风险

开源软件中被忽视的致命缺陷或全球网络基础设施大规模故障造成的风险。虽然其中部分风险将随着时间的推移大幅度减轻，比如修复漏洞和突破计算瓶颈，但其他部分

风险依然不可预测，比如可能导致部分或全球互联网中断的政治因素或自然灾害。

11 、漏洞风险或密码学加速发展的风险

密码学的加速发展或者科技的发展诸如量子计算机的发展，或将破解的风险带给CC平台，这可能导致CC的丢失。

12 、应用缺少关注度的风险

CC应用存在没有被大量个人或组织使用的可能性，这意味着公众没有足够的兴趣去开发和发展这些相关分布式应用，这样一种缺少兴趣的现象可能对CC和CC 应用造成负面影响。

13 、不被认可或缺乏使用者的风险

首先CC不应该被当做一种投资，虽然CC在一定的时间后可能会有一定的价值，但如果CC不被市场所认可从而缺乏使用者的话，这种价值可能非常小。有可能发生的是，由于任何可能的原因，包括但不限于商业关系或营销战略的失败，CC平台和所有的众售资金支持的后续营销将不能取得成功。如果这种情况发生，则可能没有这个平台就没有后续的跟进者或少有跟进者，显然，这对本项目而言是非常不利的。

14 、应用存在的故障风险

CC平台可能因各方面可知或不可知的原因故障(如大规模节点宕机)，无法正常提供服务，可能导致用户CC 的丢失。

15 、应用或产品达不到自身或购买者的预期的风险

应用当前正处于开发阶段，在发布正式版之前可能会进行比较大的改动，任何自身或购买者对CC 应用或的功能或形式(包括参与者的行为)的期望或想象均有可能达不到预期，任何错误地分析，一个设计的改变等均有可能导致这种情况的发生。

16 、无法预料的其它风险

基于密码学的 CC 是一种全新且未经测试的技术，除了本白皮书内提及的风险外，此外还存在着一些创始团队尚未提及或尚未预料到的风险。此外，其它风险也有可能突然出现，或者以多种已经提及的风险的组合的方式出现。