Capricoin+

展望未来

白皮书 v0.1

内容

Capricoin+

Capricoin+

综述

自2008年中本聪（Satoshi Nakamoto）提出的“点对点电子现金系统”概念的首次实施以来，加密货币和基于区块链的行业迅猛发展，催生了数千个不同的项目、技术和研究论文。今天，从分布式计算到企业解决方案，从医学到汽车工业，加密技术的应用已逐渐全面覆盖。

然而，资产储存的安全性仍然是人们的基本所需。此外，去中心化不依赖第三方的资金管理方式也至关重要。这就是为什么比特币在加密货币世界中屹立不倒的原因，时隔十年影响力丝毫不减。

在比特币中，跟绝大多数的加密货币一样，余额是由一系列的交易来表示的，这些交易可以追溯到区块链的最初阶段。为了信任系统，需要确保链中的每一笔交易都是有效的，并且不依赖于某个集中的实体，这也是比特币节点和矿工的目的所在。系统中的所有参与者都必须同意，以专业术语来说就是在不依赖彼此或任何人的情况下“达成共识”。系统的这种能力正是比特币理念的精髓所在。

Capricoin+

动机

最初，大家都认为比特币网络中的交易都是匿名的。交易通过生成随机的私钥和公钥对，公钥部分会形成一个可以用来接收和控制交易的地址，许多比特币用户认为，这个过程中没有任何东西可以追踪到他们的真实身份，结果证明他们错了。

借助区块链分析，研究表明交易过程中总是有数据泄漏发生。这些数据来自交易所、商家、OTC场外交易，甚至有些来自对区块链数据的收集和集聚。这样就有可能对用户进行去匿名化。像交易金额之类的数据都是公开的，数据永久存储在一个公共分类账中，一旦用户的身份被知晓，其过去和未来的所有交易以及他们的余额，就会像一个中间人会把所有东西都联系在一起，发生这样的情况就非常糟糕。因为个人和单位都希望自身的交易和余额除非给予他人权限，否则都不会想被人所知。这需要限制交易中的某些设置可见性，尽可能避免个人信息在交易中出现，以防止日后潜在的披露。

Capricoin+

摘要

本文对Capricoin+平台进行了概览，努力为大家搭建一个生态系统的蓝图。

Capricoin+是一个可扩展的隐私性很强的货币，基于Particl分叉，基于最新的比特币源，并添加了先进的功能，这意味着Capricoin+无疑在旧币的基础上更进一步，扩展和安全性方面更上一层楼。

多重隐私

隐私性（作为该币一个非常重要的特性）是通过不同的隐私级别来实现的，每个级别都有其自身的复杂性和隐私程度，当然级别因高低不同开发成本也不尽相同。

保密交易(1)：这种类型的交易（CT保密交易）采用的是机密交易的隐私协议，（创始人：格雷戈里 麦克斯韦） 该协议中，交易的金额只对交易参与者和指定的人可见，保障交易的加密完整性，但成本费用略高于标准交易。

环CT(2)：这种类型的交易（匿名交易）采用的是环CT隐私协议（也称作Shen Noether），通过结合环签名和CT保密交易协议来隐藏交易中的金额和参与者的区块链身份。它是数字货币行业的最高级别的不依赖信任度的隐私协议之一，并因Monero而知名

1 - 《保密交易》，由格雷格·麦克斯韦尔著
2 - 环CT 文献出自Noether Monero 研究实验室

隔离见证

Capricoin+本地平台采用了隔离见证，好处是所有的交易（包括私人交易）默认通过Segwit进行，扩容的同时降低交易费用。与分叉的Segwit不同的是Capricoin+的钱包地址100%与隔离见证互相兼容。

Segwit为Capricoin+平台的性能增添不少色彩，如交易中易受到攻击的保护，区块块容量的扩展，最加分的性能是Capricoin+的区块链与闪电网络相兼容。

量子电阻

当前的权益证明中发现了工作量证明中未显示出的漏洞，钱包地址的公钥会在区块被发现和签署时被暴露。对于量子计算机来说，最危险的是公钥加密的攻击。在传统计算机上，获取与比特币公钥相关联的私钥需要进行2128次的基本量子操作。如此庞大的操作运算，任何传统计算机受到攻击的几率微乎其微。但可以肯定的是，使用Shor算法，一台最够大的量子计算机只要进行1283次的基本量子操作就能破解比特币密钥。可能需要一些时间，尤其是第一代量子计算机非常慢，但仍然可行。量子计算机的隐患可能2-5年后才会发生，但任何一个项目在落地前都必须把这些隐患因素考虑在内，要在其成为问题之前杜绝，防患于未然。

请知悉公钥并不是公共地址。想要把私钥从公共地址中调换过来，要消耗无法比拟的大量能源。所以量子黑客不大可能把大量的公共地址跟私钥地址调换。当Capricoin+区块在托管节点上进行托管，传输到网络中的是在托管节点（节点内不含币）的私钥地址，而不是托管的资产。因为托管的节点可以代表任何钱包（包括热钱包和冷钱包）签署区块，而冷钱包的托管可以有效保持用户的匿名性，理论上也杜绝了量子计算机的攻击。

Capricoin+

PPoS & 静态收益

Particl的权益证明是在目前盛行的PoS3协议的基础上构建和改进的，在此基础上添加了几个安全性和实用方面的性能。

借助PPoS可获得静态收益。如果100%的币都锁定在托管服务中，那么托管奖励不少于2%，托管池中的币越少，收益就越高。举例，如果50%的币锁定在托管服务中，那么获利将不少于4%。

此外，Capricoin+平台会把产生的任何费用直接分享给托管持有者，包括但不限于货币交易、信息传递、隐私余额转账等，这意味着随着平台流量的增加，托管用户获得的收益就越高。

托管服务

托管服务是通过智能合约启动的，用户把权益授权给“托管节点”，而托管节点中不含任何币。这些“托管节点”的任务是提供可连接到Capricoin+区块链的专用资源，充当钱包的角色不允许动用货币的前提下管理资产。

托管服务节点旨在与硬件和多重签名的地址相结合，允许“离线”的货币在没有风险、不容易被黑客或使公钥暴露到网络中的情况下进行托管。托管节点可在任何设备上部署，无论是公共或是云服务器，虚拟机或DSD都是可行的。

去中心化投票

把PPoS整合到区块链投票系统中，所有Capricoin+用户都可以进行投票。该功能有效地促进社区用户达成共识并更好地协调自身。

投票在一定数量的区块中进行，每个区块都是一张选票，也就说发现的区块越多，其选票就越多。托管者可以进行任意数量的投票，一旦托管者找到区块，他就可以为某个特定的选项投票。

在PPoS中的投票制度中，用户如果没有进行托管不具备投票的资格，决定权将留给社区的用户。

数据储存网络

数据存储网络用于存储Capricoin+的任何数据(如：跟开放市场相关的数据、图像)。平台不用在乎使用了多少数据，从而很好地扩容。

DSN是用于描述一组用于在互联网上存储和检索数据的特定软件的专业术语。DSN专业术语是一个抽象的概念，不需要知道特定的DSN内部如何运作，只要它能够存储Blob的数据随后使用类似的加密标识符进行检索。目前盛行的DSN包括BitMessage、IPFS、SMSG、HTTPs、TOR等。

在DSN上存储数据时，哈希内容会在Capricoin+区块链上随之创建。为了验证从DSN检索获得的数据完整性，哈希值会被重新计算，继而跟存储在Capricoin+区块链上的进行比较。如果哈希值匹配，则数据可信，若不匹配，则会被平台拒绝。

共识机制兼容的可延展性

当今科技的发展突飞猛进，很多共识协议因其之前没有考虑到扩展性而无法经受住时间的考验。能长期存活的共识协议自身应足够稳健、灵活，若要进行升级扩展的话，开发人员不费吹灰之力方可实现。数据存储网络(如：DHTs、BitTorrent、IPFS)和区块链解决方案的发展始露苗头，还没有任何模范的"赢家"标准，也许以后也不会有，所以共识协议必须顺应时代、科技的发展。

Capricoin+应运而生，与时俱进。该平台的设计初衷是为了能够与任何DSN和数据之间的互换，而不是因文本内容或用户喜好每次都使用一成不变的硬编码DSN。

通讯安全性

安全的通讯（SMSG）是Capricoin专属的DSN，是一个去中心化的P2P消息混合网络，每个人的端到端加密消息和数据的副本会被储存到节点，时长48小时（可增加费用延长储存时长）。这是系统的默认设置，平台上的DSN也是很隐私的。该操作是参考C++语言开发的，后台运作跟Capricoin+区块链一样都是点对点进行的。

所有节点会不断尝试对每条传入的消息解密，但只有在节点能够重新计算所述的消息附带的HMAC哈希时才能成功。如果哈希检查失败，该节点则无法对其解密，这意味着该消息要么是伪造的、被篡改的，要么是针对另一个节点的。因为SMSG消息和数据绝大多数是从整体元数据中剥离出来的，诸如IP地址、发送者或接收者等信息是无法被人为提取的。元数据就是哈希、加密的有效负载和临时公钥附带的在SMGG上的数据。

隐私智能合约

Capricoin+正在部署高安全性的智能合同，因其复杂程度还未完成。好消息是Capricoin+的开发市场含MAD托管机制（将在2020年第三季度面世）。任何开发者都可以在Capricoin+上创建自己的Dapp，签订保密交易CT和环CT隐私协议保障用户的隐私权。

社区管理

围绕去中心化的原则，Particl不由团队或第三方管理，而是由其托管者社区监督管理的。考虑到Capricoin+开放市场这个功能是全匿名的，一些不受欢迎的产品或服务很可能会挂牌出售,所以为了保护其合法性和避免不道德或非法活动的发生，对开放市场的监管至关重要。若第三方被提名为“调解人”会带来很多如法律责任、集权制、缺乏延展性等诸多问题。

去中心化的隐私市场

Capricoin+的去中心化市场的扩展性很强，可作为安全的电子商务解决方案。以隐私为核心，为贯穿平台的在线购物和销售产品/服务打造全套工具。

Capricoin开放市场的建设始终以隐私为核心，这意味着买家和卖家之间的所有交易是可替代的（不可追踪、私密）。为了实现这一壮举，会部署许多隐私解决方案，如CT托管智能合约、IP模糊处理、消息加密和元数据泄漏保护。

去中心化托管：由于买方和卖方彼此不了解、互不信任，除非建立一种约束机制，否则就无法防范某一方的违约。常见的惯例是：开放市场和支付程序处理器选择相互信任的第三方（通常是平台本身）作为“托管代理”。但是，这不仅引申出延展性和隐私问题，也无法提供任何保护措施防止托管代理和某一方之间的勾结。Capricoin+是一个完全去中心化的解决方案，处理类似这样的问题，Capricion+不需要第三方的干涉，一个名为“MAD 托管”的智能合同就能搞定，好处是这种类型的托管并不需要支付任何费用。

博弈论：共同毁灭原则（MAD机制）是一种“俱皆毁灭”性质的军事战略思想。此思想假设双方或多方都有足以毁灭另一方的武力，而且一方如果受到另一方攻击，不论什么理由都会以同样或更强的武力还击。对立的两方或多方中如果有一方全面使用核武器则两方都会被毁灭。

它基于威慑论和纳什均衡论，理论认为：对敌人使用强大武器的威胁会阻止敌人使用同样的武器反击。这是纳什均衡论的一种形式，如果一旦打斗起来，任何一方都不会主动挑衅彼此或放下武器。Capricion+的MAD托管机制相当于共同毁灭博弈论中的核毁灭威慑因素，如果一方有违约 行为，那么双方都会遭受经济损失。

工作原理: MAD托管合同中，Capricoin+使用的是BIP 65作业码，该作业码将资金锁定在一个安全的多重签名地址，直到所有各方在交易上签名方能完成，从而互相制约。

鉴于交易的诚意，卖家要先预存一笔押金，象征着虚拟化的握手，下称握手价格。押金价格可以是产品价格的任意%，若要达到可实现的MAD几率，最好是预存产品100%全款。然后，买家预存等值的握手价格，加上产品的自身价格。在双方彼此确认交易完成之前，托管资金不会向任何一方释放。为了避免拖延发生，MAD智能合约有一个定时器，可事先设置好交易时长（如果双方都同意，可延长交易时间），随后资金会被销毁（这里的销毁是指永远锁定，双方都没有解锁的权限）。这可以防止双方在托管过程中的故意拖延或妨碍。

若交易双方对交易没有异议，双方都需要确认交易已完成。该操作完成后，产品的托管资金将释放给卖方，保证金会以Capricoin+退还，不收取双方任何费用。

隐私性：Capricoin+的MAD托管系统赋予了开发市场替换性，因为它使所有交易在默认情况下无法追踪。事实上，不仅整个开发市场的内容进行了DSN级别的加密，而且所有货币交易采用保密交易（CT）而变得不可追踪。因为MAD托管智能合约只与保密交易（CT）工作，并强制所有的交易必须通过它来实现。如果保密交易（CT） MAD 托管机制可取，那么凭借此技术可增强更多的隐私性，因为它使得所有在开放市场的交易都一样（可替换）。

MAD托管机制的隐私加强另一个方面是它缺乏作为托管代理的第三方。事实上，在大多数涉及第三方的托管制度中，双方当事人需要跟仲裁员一同讨论，让交易的每一个细节都了解到位。万一出现任何问题，托管代理就可以介入，根据以往的谈判记录提出解决方案。这涉及到对仲裁人的极大信任，不需要第三方干预的前提是仲裁员不偏不倚的立场。

隐私发布: 虽然公开的发布可以由Capricoin+社区管理，但是隐私发布不能。隐私发布是一种私密的发布形式，只有密钥权限的用户才能访问。在开发市场的公开部分是不可能找到这些发布的。

反垃圾邮件发布费用: 垃圾邮件是所有网络的痛点。为了减少Capricoin+开发市场出现垃圾邮件的可能性，采取了以下这两个措施: 上市费和续期费。

开发市场数据存储: 数据以链外的方式储存在DSN上。Capricoin+上的默认DSN是SMSG，SMGG是最好的隐私规范。把开发市场的数据以链外方式储存的好处是少占Capricoin+平台的容量，不会造成其他区块链的膨胀或给中心节点以及主节点带来不良影响。大多数上传到DSN上的内容会产生一个可储存在Capricoin+区块链上的小哈希。以后这个哈希在DSN检索内容时必须要与之前检索内容的哈希匹配，否则，这些内容会被会列为诈骗类从而被Particl平台拒绝。