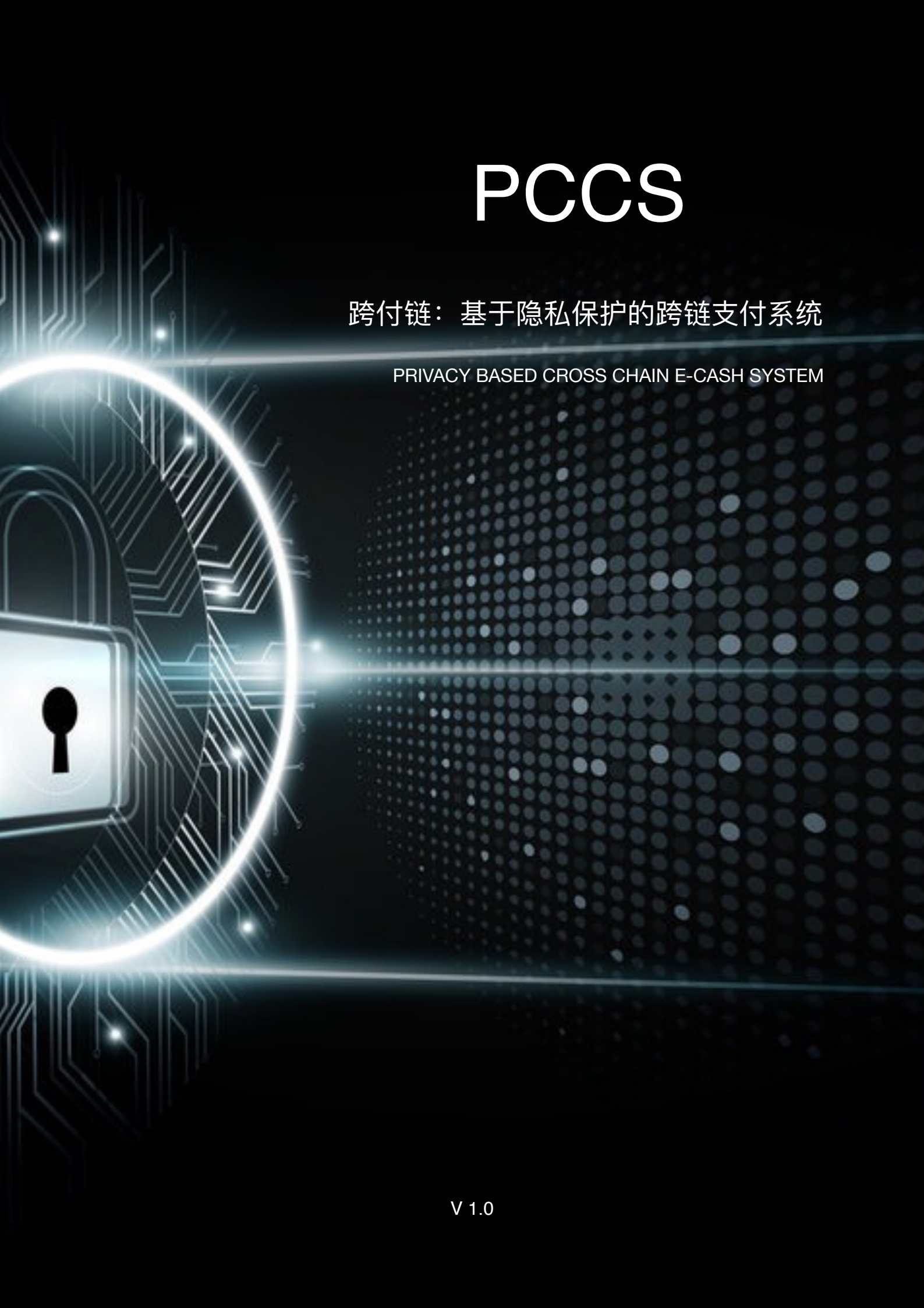


PCCS

跨付链：基于隐私保护的跨链支付系统

PRIVACY BASED CROSS CHAIN E-CASH SYSTEM

V 1.0

目录

一、背景

比特币自2009年诞生以来，作为一种电子现金货币已经成为社会现象级话题，开创了去中心化加密货币的先河，其底层技术区块链更是不断被人们所研究。作为区块链2.0的以太坊则摆脱了数字货币的枷锁，创造性地提出了“可编程区块链”，使其成为去中心化应用开发的平台，带来了深远的影响。

以匿名性著称的零币和门罗币同样取得成功。自比特币诞生近10年以来，数以千计的区块链项目被开发出来，有的项目从商业落地角度出发，希望借助区块链的特性寻求商业场景，也有的项目从解决区块链性能问题出发，希望开发性能更可靠、可用性更强的区块链。 但是目前大多数区块链项目仍然因为区块链技术架构限制面临着诸多难题，如区块容量扩展性和伸缩性、缺乏链上治理、分布式共识性能瓶颈等。

我们认为这些问题不仅存在于某一条区块链，也不仅局限于某一种应用场景上，所以我们在研究和尝试解决这些问题的时候，发现诸多问题不是单一区块链能彻底解决的，而是应该探索系统化的多链解决方案，让各种同构或异构区块链能够互联互通，取长补短，价值互换。于是我们发现跨链技术的设计和实现，是解决区块链诸多问题的关键。无论对于公有链还是联盟链，跨链技术都是实现价值互联网的关键，它是把区块链从分散的价值孤岛中拯救出来的良药，是区块链向外延展和互联的桥梁，能进一步拓宽区块链技术的应用范围。

1.1 用户隐私

当前，大众对隐私保护的关注和需求日益加剧，许多家知名公司都先后被曝光出泄露了大量用户隐私数据，有YAHOO、UBER、Paypal、信用机构Equifax、英国国家医疗服务体系（NHS）等等，相关泄露数据涉及几千万到数亿规模的用户。

脸书也因为2018年发生的最大规模的隐私泄露事件，导致市值在两天内蒸发掉数百亿美元，并有可能面临达其四倍市值的天价罚款。隐私问题同时也引起了很多国家政府的重视，欧盟率先颁布《通用数据保护条例》(GDPR)就是一个旨在为了督促各家公司有效保护用户隐私的法案。

互联网高度发展的现在，给我们带来了诸多便利，同时将个人隐私数据的安全保护的需求推上了一个新高度，互联网应用场景中大部分的隐私泄漏往往是由于高度集中化的平台缺乏足够的数据安全保护机制引起的。所以大家都意

识到需要一种新的安全机制来辅助或改变这种高度集中化的数据储存模式，在这个探索的过程中，一种新的安全机制的诞生为解决数据隐私问题提供了可能性－区块链系统。这个被认为能从根源上杜绝此类事件发生的安全机制早在09年就已经被分享出来了，随着区块链的发展，大家发现比特币和以太坊等区块链网络的设计其实并没有充分考虑当去中心化网络与使用者现实身份结合后，区块链上存储的用户数据会产生用户的隐私泄漏问题。区块链网络中数字资产及其交易记录等异常敏感的信息，对所有人透明并且是不可篡改的，当区块链在现实场景中进行大量的应用的真正落地时，区块链数据与现实使用者一对一映射的关系也被暴露，这样对大部分场景需求和使用者来说，无疑是很难接受的。

隐私权是法律赋予我们的神圣的权利，我们应该有非常清楚的认识。再比如财务隐私，财务隐私合法使用案例的范围很广。财务隐私对于世界上发生的大多数交易来说应该是必须的，数字货币相关账户的资产和交易的隐私数据通过区块链上存储的交易记录暴露在所有人面前是不合理理的。

在智能合约中，整个行为序列通过网络传播并记录在区块链上，所以是公开可见的，许多个人和组织认为金融交易（例如保险合同或股票交易）是高度机密的，比如多方之间基于某些条款的细节产生的交易，原本可能需要当事人的信息保护，现在却无法做到。所以，缺乏隐私是广泛采用去中心化智能合约的主要障碍，隐私保护技术的匮乏已经成为了去中心化应用普及落地的严重瓶颈，故而相关领域的技术发展进程也备受公众关注。

1.2 BlockChain隐私泄漏风险

最早出现的Bitcoin网络是典型的区块链技术代表，是目前市场上主流的加密货币，后起之秀以太坊及EOS几乎都基于Bitcoin相同的技术特点开发的，下面我们分析一下比特币网络可能存在的隐私泄漏的风险。

首先从比特币交易系统的结构设计来看：

交易数据的UXTO模型包含输入地址和输出地址信息，每一个输入地址都指向前一笔交易，所有输入资金都能够追溯到产生的源头。在共识过程验证节点需要检索历史交易，所有的交易信息没有采用加密等手段保护数据。

比特币交易参与方的地址都是由用户自行创建且与身份信息无关的，任何人都无法直接通过观察交易记录推测出交易中用户的身份信息。但全局账本公开的交易之间存在关联关系，潜在攻击者可以通过分析全局账本中的交易记录推测出比特币地址的交易规律，包括相关地址的交易频率、交易特征、地址之间的关联关系等。基于这些规律律，攻击者有可能将比特币地址和特定用户在真实世界中的身份相关联。

其中一种方式主要通过分析地址相关的交易记录，获得该地址交易的规律律特征，据此推测对应用户的身份信息。由于在某一特定类型的区块链交易中会存在它特有的交易特征，攻击者可以根据地址的交易特征，对其交易发生的真实场景进行还原，从而做出用户真实身份的推测。Androulaki E.等人设计了了一个匹配区块链地址与学生身份的模拟实验，学生以比特币作为日常交易的支付手段，并使用比特币推荐的一次性地址方法加强隐私保护，分析人员通过基于行为的聚类技术，能够以42%的准确率将学生身份和区块链地址成功匹配。Monaco J. V.等人将比特币用户的交易行为进行量化，以交易时间间隔、资金流向等12个维度为依据分析用户的交易规律，经过6个月实验得到的大量量数据表明，利用这种分析模型成功识别用户真实身份的精度高达62%，错误率低于10.1%。

1.3 隐私保护技术

我们很高兴地看到现在有一些团队开始关注到去中心化网络的隐私保护问题，比较著名的项目包括Zcash，门罗币和达世币。

一种广泛应用的方法是在不改变交易结果的前提下改变交易过程，使攻击者无法直接获得交易的完整信息，这种方法被称为“混币”。譬如在Chaum D.的文章里提到了一种匿名通信技术，在通信过程中隐藏了真实的通信内容，基本思想可以通过式(1)表达:

$$CM\ (Z1,\ CA\ (Z0,\ m),\ A)\ -\!>\ CA\ (Z0,\ m),\ A \quad (1)$$

Ê (1) 左侧为发送方发给中间人的信息，右侧为中间人将信息处理理后发送给接收方的消息。发送方想要将消息 $Z0$ 和发送给接收方的地址A，首先使接收方的密钥 $\mathbf{C}A$ 对消息进行加密得到 $\mathbf{C}A\ (Z0,\ m)$，然后将中间人的验证消息 $Z1$、加密后的消息 $\mathbf{C}A\ (Z0,\ m)$和接收 方地址 A 进打包，并使用中间人的公钥 $\mathbf{C}M$ 进行加密，防止信息在发送过程中被攻击者截获或篡改。中间人收

到信息后使用自己的私钥进行解密，得到 $Z1$，$\mathbf{C}A\ (Z0,\ m)$，A，但无法解密 $\mathbf{C}A\ (Z0,\ m)$ 的内容。中间人在验证 $Z1$ 无误后，将 $\mathbf{C}A\ (Z0,\ m)$ 发送给地址 A 。接收方使用自己的私钥解密消息，完成此次通信。

利用这种方法，消息没有在发送者和接收者之间直接传递，而是通过中间人间接传递，使攻击者无法观察到真实发送者和接收者之间的通信行为，提高了通信的匿名性。若将消息通过多个中间人进行传递，攻击者发现双方通信关系的难度将大大增加。

数字货币中的混币机制借鉴了了上述思想（如DASH和门罗币），通过中间层级结构，切断交易中真实的发送方和接收方的被可追踪的关联。混币过程的执行可以由可信的第三方或某种协议实现。根据混币过程中有无第三方节点参与，可将现有的混币机制分为两类：基于中心节点的混币机制和去中心化的混币机制。这两种机制在混币可靠性、混币效率和混币成本等方面各有优势和缺陷。

不过随着技术的发展，更为尖端的加密学的技术被应用到区块链隐私保护中，譬如 Zcash 对零知识证明的应用。

1.4 跨链的意义

区块链领域现在除了创世纪的Bitcoin以外，已经出现百家争鸣的景象，多种功能性的加密数字货币，以BTC为代币的数字黄金、以ETH、EOS为代表的公链Token、以及以XRP、XLM为代表的跨境结算货币成为数字加密货币的主要参与者（更多的山寨币也可能加入的这个竞争环境中来）。目前，加密货币的兑换技能通过交易所进行，大大限制了加密货币价值交换的效率，成为区块链技术发展的一个瓶颈。

所以，跨链技术的研发是迫在眉睫的重中之重，打通多链，实现多链并行，才能更大的服务用户，服务社会，服务全球。

跨链的最大的价值莫过于实现高效的数字加密货币的兑换，就是无界限的、安全的、实时的跨链支付。并且解决多链分布式协作问题，越来越多的人在多链生态中形成跨链共识，支持跨链支付，实现跨链场景，落地跨链应用。还有分布式多链的链上治理，最终打造一个伟大的跨链生态。

1.5 PCCS概述

多链并行，之所以目前不被社区过多提及，是因为技术实现上存在巨大难度。维护几条独立运行的区块链网络，可能仅仅需要投入数倍的基础设施资源。 而要使这些链相互之间能够去中心化、安全可靠地持续互操作，构建多链系统的全局一致性状态视图，就必须设计与区块链底层机制协作的跨链通信模型。 值得一提的是，EOSIO软件层面，已经考虑到了跨链友好性，包括轻客户端验证的Merkle证明、跨链延迟和最终性、完备性证明、隔离见证。

我们研究发现，以往的跨链项目都是试图先去解决异构区块链之间的跨链问题，如比特币和以太坊之间的跨链通信。然而现实是这些跨链项目的落地应用并没有被广泛接受，缺乏充分的性能验证和安全验证。 我们认为，实施跨链的前提是区块链内建了友好的跨链机制。EOSIO在设计之初就考虑到了为跨链提供相关数据结构的支持。未来会有很多公链运行在开放网络中，也会有很多联盟链、私有链运行在联盟或企业的内部网络中，这些区块链其实可以构建于同一套EOSIO软件设施之上，差异仅存在于应用层。通过开发第一条可与EOS主链进行跨链互操作的并行链，PCCS将承载各种超大型去中心化商业应用的落地，并且衔接形态各异的联盟链、私有链，充分发挥多链并行的无限扩展性优势，帮助EOS生态真正领衔区块链3.0时代。

作为EOS主链的第一条协作并行链，我们将在EOSIO软件基础上进行跨链技术的系统功能定制、插件开发、合约部署，邀请社区成员广泛参与竞选超级节点， 维护并行链运行。PCCS将尊崇EOS宪法精神并考虑EOS ICO投资人的利益分配和投票权，但在系统参数上将稍微有别于EOS主链，以支持同构跨链和更远将来的异构跨链。

另外，PCCS还有一个非常重要的特征—隐私保护。在区块链的交易过程中，账户体系和交易的过程，以及交易的数额等重要信息进行了特殊处理，以达到保护使用者隐私的目的。PCCS的隐私保护特征如下：

不可追踪性：在区块链的网络中的每一笔交易都具有输入和输出，如此一来就构建了一个有向无还图，在这个图上可以跟踪所有的交易流向。在我们的设计中将打断交易链接，使攻击者无法追踪。

不可关联性：通过加密技术手段使收款地址无法被关联破解。

抗统计分析：我们通过技术手段将地址以及地址之间的关系完全隐藏。

可选择的审计方案：用户需要有一个完全信用的第三方对他发生的交易进行财务方面的审计时，可以做出选择，决定是否给予第三方一个跟踪他所有交易具体信息的能力。

1.6 公链概述

ETH概述：

以太坊（Ethereum）是一个建立在区块链技术之上，去中心化应用平台。它允许任何人在平台中建立和使用通过区块链技术运行的去中心化应用。

区块链是从比特币衍生出来的，一般我们称为区块链1.0，主要以各种特色的电子货币为主，最多的行业应用是小额支付、外汇兑换等等。而随着区块链的发展，有了区块链2.0。区块链2.0相比于区块链1.0来说应用场景也更为丰富，不仅仅局限支付，也可以包括股票、债券、期货、贷款、抵押、产权、智能财产和智能合约。

比特币是区块链1.0的代表，以太坊是区块链2.0的代表，以太坊是个平台和编程语言，包括数字货币以太币（Ether）和以太脚本（EtherScript），用来构建和发布分布式应用。以太坊是个基础性的、开放的通用数字货币平台来实现图灵完备虚拟机，可以运用任何货币、协议和区块链。定位来说以太坊旨在成为一个平台，而比特币则是一个货币体系。

以太坊是个平台和编程语言，包括数字货币以太币（Ether）和以太脚本（EtherScript），用来构建和发布分布式应用。以太坊是个基础性的、开放的通用数字货币平台来实现图灵完备虚拟机，可以运用任何货币、协议和区块链。

以太坊具备开放通用特性，网络的每一个节点都可以运行以太坊虚拟机来发布分布式智能合约程序。以太坊智能合约，能够调用多个其他区块链、协议、货币。作为与底层区块链和协议无关的通用分布式运用开发平台，具备了成为一个平台级产品的条件。

以太坊的分布式系统

以太坊有自己的分布式系统：包括文件服务Swarm、信息传输Whisper和信誉担保。Swarm是个去中心化文件服务；Whisper是加密通信传输系统；信用

担保提供去信任网络中建立信誉和降低发现的系统，可以由Crypto Schwartz和TrustDavis等第三方提供。

EOS概述：

EOS是Block.one主导研发的一个底层公链系统，目的是解决现有的区块链应用性能低、安全性差、开发难度高以及过度依赖手续费的问题，实现去中心化应用的规模性扩展。

作为下一代公链的代表性项目，EOS已经于2018年6月份在社区成员的共同努力下成功启动了主网，吸引了区块链行业内外的广泛关注。 我们认为，随着Block.one开发团队在EOSIO软件开发上的持续努力，以及超级节点们在主网运维和安全上的经验积累，EOS主网在2018年年底前将逐渐稳定，并迎来DAPP爆发期。 然而，即使当前超级节点都配备了顶级硬件，但仍受限于单线程执行模型和非JIT的WebAssembly虚拟机，EOS主网TPS在几百到一千。 我们很早就注意到，EOSIO白皮书摘要中宣称EOSIO软件引入的全新区块链架构设计，能够通过纵向和横向扩展，最终达到百万级TPS。 纵向扩展，包括不断升级硬件性能、引入多线程执行模型和JIT使能的WebAssembly虚拟机，我们相信将使TPS推高到一万左右。 我们认为，只有通过横向扩展，即采用多链并行的方式，EOS才有可能达到百万TPS，而那时，我们所看到的EOS已经不是一条主链，而是无数个使用EOSIO软件的并行链组成的EOS同构跨链群。

二、匿名隐私

2.1 背景

比特币是第一个实现广泛采用的数字货币。该货币的增长部分归因于这一事实，与传统的电子现金计划不同，它不需要信任方。比特币不是指定中央银行，而是使用称为区块链的分布式账本来存储用户之间进行的交易。由于块链被相互不信任的同行大量复制，因此它包含的信息是公开的。

虽然用户可能会使用许多身份（或假名）来增强他们的隐私，但越来越多的研究表明，任何人都可以通过使用区块链中的信息对比特币进行去匿名化，例如交易图的结构以及交易的价值和日期。因此，比特币甚至无法提供传统支付系统提供的一小部分隐私，更不用说匿名电子现金计划的强大隐私了。

2.2 痛点

为了保护使用者的隐私，用户因此需要即时、无风险，并且最重要的是，自动保证他们的朋友、同事以及他们交易的商家无法公开的他们的消费习惯和帐户余额的数据，匿名交易还确保Token的市场价值与其历史无关，从而确保合法用户的token保持可替代性。

Zerocoin扩展了比特币以提供强大的匿名保证。与许多电子现金协议一样，Zerocoin采用零知识证明来防止事务图分析。Zerocoin不是一种完整的匿名货币，而是一种分散的混合体，用户可以通过Zerocoin协议定期“清洗”他们的比特币。

门罗币引入了一个新的技术就是环签名技术，虽然环签名在其之前就提出来了，当在当时并不叫做环签名，而是叫做群签名（Group Signature）。但是这样的环签名在现实使用场景中需要可信的第三方参与，第三方仍然为中心化的机构，仍然有可能出现作恶情况。

最新的Beam、Grin项目使用了新的技术MimbleWimble开启了新一波隐私方案的讨论。虽然在技术实现上有更佳的隐私性、实用性、延展能力。但是在安全方面是否一定超越以往的方案呢。我们还需要更深入的研究和发现。

那我们我怎么样在更加复杂的实际场景下去应用我们的隐私保护机制呢？我们的区块链世界发展的未来，可能出现多个深耕某些行业的公链，更有专业服务某些场景的区块链。所以未来的隐私和支付还需要一个关键技术加持，这就是大家一直讨论研究的跨链技术。

隐私的保护的应该是支付应用，支付的技术的基础是万链互联下的跨链技术。

2.3 我们的设想

（1）引入分布式匿名支付方案的概念，该方案具有强大匿名保证的完整分散式电子货币的功能和安全保障。并在特定的加密假设下证明了它的安全性。该结构利用了零知识证明领域的最新进展。

（2）通过一个称为EOScash的系统实现分布式匿名支付方案。

为了验证系统方案，我们通过在1000个节点的测试网络中进行实验来测量其性能并建立可行性网络。这样我们就可以作为比特币的分支部署，并以相同的规模运行。

三、跨链通信协议

3.1 可行性概述

跨链技术包括链间互联互通，链上资产在链间共识和同步的基础上可达成原子交换，来源链资产仍具备目标链链上属性（如可权益证明、可跨链执行合约）。

为实现以上跨链技术所要求的功能，我们需要把跨链技术作为一个完整的系统去研究，让跨链技术不仅服务于链上资产证明，更要利用跨链技术去实现区块链连接性、伸缩性、扩展性，使跨链技术作为推进区块链项目落地的一种绝佳方式。

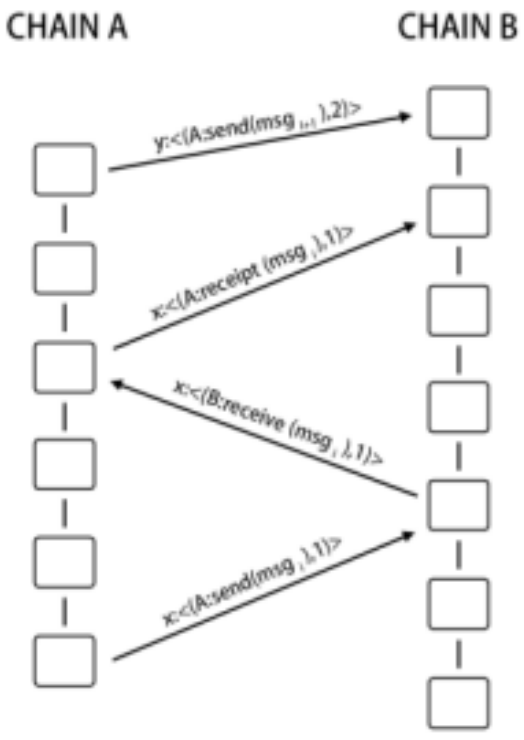
从实现跨链机制的角度来看，我们需要做的工作有：选择对跨链友好并支持智能合约虚拟机的区块链系统，定义链间通信方式，使用合约创建链间通信协议包、解析协议包、跟随和验证区块头；定义链上资产转移的形式，使用合约创建、锁定和销毁链上资产。

我们这里定义一种典型的跨链交互形式：

1. 链A需要构造一笔跨链交易/执行链B合约请求

2. 这笔跨链交易需要被中继转发到链B

3. 链B需要验证交易合法性/请求合法性并回执给链A



4. 链B存储这一笔跨链交易

3.2 协议设计

我们现在根据链间通信的场景来讨论如何实现链间通信。

首先我们需要设计一种跨链通信协议ICP（Inter-Chain Protocol）。ICP协议使用跨链消息传递模型，不对网络同步做任何假设，即先不考虑网络问题。协议需要能构造跨链交易，使中继者能够将其从一个区块链中继到另一个区块链。链A和链B需独立地确认新块，并且从一个链到另一个链的协议包可以被任意延迟或检查。协议包传输和确认的速度仅受各区块链本身速度的限制。这里定义的ICP协议不感知载荷。链B上的协议包接收者根据接收到的信息决定如何采取行动，并根据协议包包含的数据可以添加其自己的应用逻辑来确定要改变哪些状态事务。

为了促进有效的ICP协议传输和确认，我们定义ICP信道：一组可靠的消息队列，可以保证ICP数据包的跨链因果排序。因果排序意味着如果数据包x在链A上的数据包y之前被处理，则数据包x也必须在链B上的数据包y之前被处理。

$$A{:}send(msgi) \rightarrow B{:}receive(msgi)$$

$$B{:}receive(msgi) \rightarrow A{:}receipt(msgi)$$

$$A{:}send(msgi) \rightarrow A{:}send(msgi+1)$$

$$x \rightarrow A{:}send(msgi) \Rightarrow x \rightarrow B{:}receive(msgi)$$

$$y \rightarrow B{:}receive(msgi) \Rightarrow y \rightarrow A{:}receipt(msgi)$$

ICP信道在两条区块链间实现了一个分布式向量时钟去添加两条链处理消息的约束条件，保证链间的每一笔交易都具有明确的因果关系和时序性，这样就不会因为网络延时、链间共识不同而存在状态不明确问题。

当一个特定的ICP数据包被提交给链B时，链B接收数据包并创建资产凭证，并要求链A再发送一份确认链B上资产凭证已生成的回执证明。

3.3 数据结构

下面我们详细讨论使用ICP协议完成跨链通信过程中所涉及的协议包及其相关功能的数据结构。我们需要定义两种ICP协议包，第一种可以生成跨链交易的数据包，第二种可以验证两条链的状态机的回执数据包。

3.3.1 交易数据包

交易数据包包含：

- 路由信息 (route)：路由信息里包含了中继者需要解析并中继的路由字段
- 序列号 (sequence): 序列号是一个无符号的任意精度整数
- 发送方信息 (sender): 来源链的唯一标识、连接信息等字符串
- 交易数据 (tx data): 交易方的交易和链上证明
- 接收方信息（receiver）: 目标链的唯一标识、连接信息等字符串

3.3.2 回执数据包

回执数据包包含：

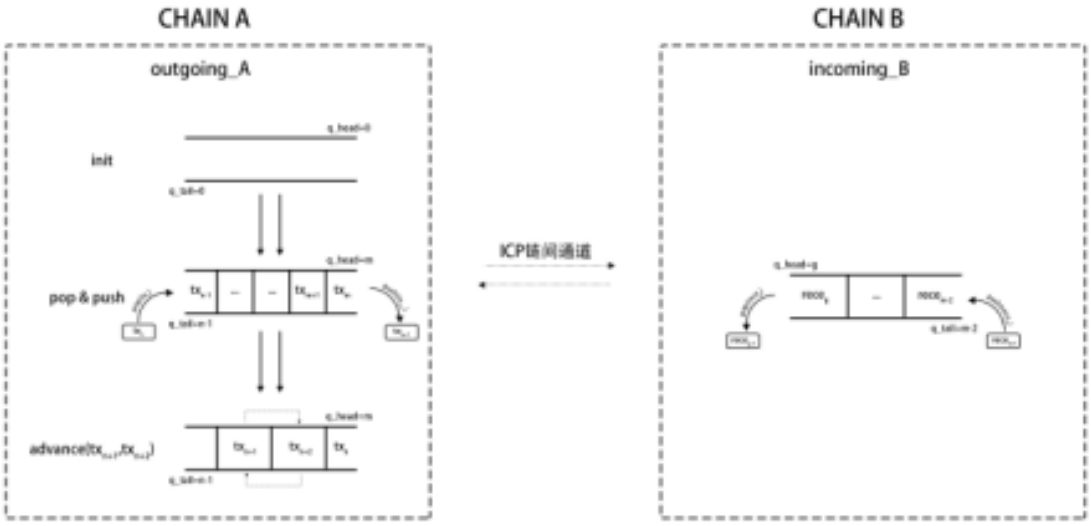
- 路由信息 (route): 路由信息里包含了中继者需要解析并中继的路由字段
- 序列号 (sequence): 序列号是一个无符号的任意精度整数
- 发送方信息 (sender): 来源链的唯一标识、连接信息等字符串
- 接收方信息 (receiver): 目标链的唯一标识、连接信息信息等字符串
- 返回结果 (result): 目标链的接收处理证明

3.3.3 链间信道

为了实现严格的交易消息排序处理方式，我们还需要引入消息队列，需要实现以下队列操作：

- outgoing_A: 从链A发送到链B上的ICP交易数据包，存储在链A上
- incoming_A: 链A回复的对链B的ICP交易数据包的回执数据包，存储在链A上
- outgoing_B: 从链B发送到链A上的ICP交易数据包，存储在链B上
- incoming_B: 链B回复的对链A的ICP交易数据包的回执数据包，存储在链B上

ICP链间信道促进两个区块链A和B之间的有序双向通信。ICP链间信道需要独立处理自己队列头部初始化和更新等操作。



四、PCCS跨链技术演进

4.1 同构跨链

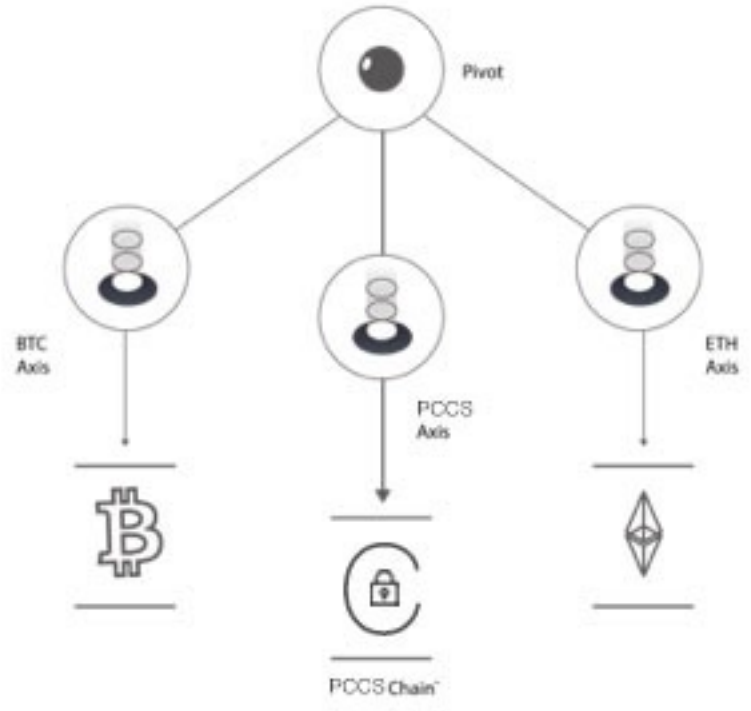
PCCS作为EOS主链的并行链，将EOSIO软件作为区块链底层基础设施，依然保持同样的BFT-DPOS共识机制和区块链数据结构。因此其与EOS主链之间的跨链，属于同构跨链。同构跨链的难度在于必须深刻理解其同构链的底层

机制，并在不影响保持主链独立性的前提下，通过编写插件和智能合约来实现同构跨链协议包的传输、解析、处理。

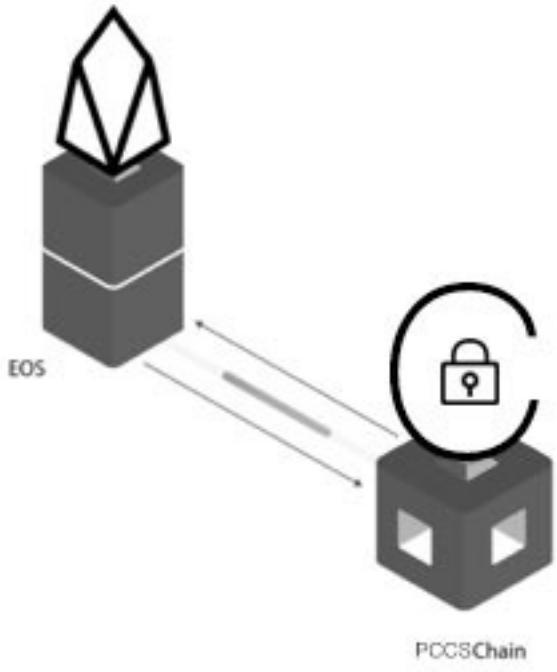
4.2 异构跨链

PCCS更远期的目标是，接入PCCS-Chain跨链生态，实现与各主流公链的互联互通，包括比特币、以太坊、Cosmos、Polkadot、Filecoin等，也通过PCCS可以实现EOS同构跨链体系与外界各公链的互联互通。显而易见，这种异构跨链，由于要考虑不同的区块链的机制细节差异，难度比同构跨链高得多。

我们将会以现有的异构链跨链技术为研究落脚点，如Cosmos、Polkadot，通过实现特定的平行链、区域链与各公链、联盟链、私有链进行跨链交互，通过对这些跨链技术进行深入的研究和升级，独立探索出一种更安全、扩展性更强、链间通信性能更强的跨链技术。PCCS-Chain异构跨链的互联互通，将可能采用中继链、区域链、平行链等的方式进行探索研究。



针对PCCS，我们将会设计这样一个类似于区域链的EOS Axis，实现它们之间的跨链通信。从而，EOS主链和其同构跨链体系将通过PCCS Chain并行链和EOS Axis区域链，与PCCS-Chain Pivot枢纽链互联。这样以PCCS-Chain



Pivot为中心的跨链体系，可实现最为广泛的公链互联互通、价值流动、资源互操作。

五、PCCS设计与实现

通过以上对区块链间通信协议的深入研究，我们定义了同构跨链与异构跨链两个概念，并将PCCS与EOS主链的跨链通信分类到同构跨链体系的范畴进行研究和开发。

PCCS并行链与EOS主链之间的同构跨链，涉及以下组件：

- 同构跨链协议（Isomorphic Inter-Chain Protocol, ICP）
- 同构跨链合约，在并行链和主链上同时部署，支持跨链协议包的解析、跨链交易的验证和执行，以及EOS原生币（EOS）、PCCS原生币（PCCS）的跨链资产转移
- 同构跨链通道，通过逻辑证明确保通道建立的稳定性和安全性
- 中继者，将跨链协议包在并行链和主链之间安全快速地传输

PCCS在不远的将来，还将参与到PCCS-Chain异构跨链生态中，作为连接EOS主链和异构跨链网络的桥梁。PCCS-Chain异构跨链网络，将广泛容纳和连接全球最前沿主流公链，使得形态各异、应用场景千差万别的异构链之间的直接通信成为可能，构建多链高速公路网络。PCCS也将因为这样纽带性的角色地位，不仅大大提升自身价值，也促成EOS生态和其他公链生态的紧密融合与协作。

PCCS并行链采用EOSIO软件，做若干系统参数修改或功能增强，与EOS主链将有且仅有如下提及的差异，除此之外，拥有EOS主链的其他所有特性或功能，包括BFT-DPOS共识算法、基于权限控制的命名账户体系、智能合约等。

5.1 同构跨链协议（Isomorphic Inter-Chain Protocol）

跨链协议是为了能够表达去中心化的跨链互操作过程中的状态转换。同构跨链协议仅需要考虑同构链之间的互操作，是一种对称、双向的协议。基于尽量避免改动EOSIO软件底层设施的出发点，我们将实现同时部署到两条同构链上的跨链合约。因此，同构跨链协议被设计为包含状态数据和区块证明的数据包，由中继者执行链与链的数据包中继，也即调用跨链合约的接口。

协议数据包的设计，需要考虑：

• 可证明性：被中继的数据包必须在来源链上写入区块，并通过Merkle证明来表达其不可篡改，使得目标链可以安全地将它作为依据来执行状态转换。

• 最终性：一个数据包被中继到目标链并生效时，其来源链的相关区块必须已被确认、不可逆，否则跨链共识失败。

• 全局顺序唯一性：确保数据包的因果顺序，且避免重放攻击。

• 中继幂等性：多个中继者可能重复中继同一个数据包，必须保证只有第一次中继生效，后续中继均不产生任何效果。

• 超时可控性：由于网络通信延迟或拥堵、中继者不及时中继或因故障暂停中继，总会不可避免地造成数据包的中继延迟，这时需要超时机制来表达跨链交易发起方对于瞬时成功或失败的诉求。

我们设计用于PCCS并行链和EOS主链的两种跨链协议包：ICPBlockHeader和ICPTx。

ICPBlockHeader是用于一条链同步跟踪另一条链的区块（头）的跨链协议包，形成跨链交易的安全证明链条：

```
struct block_header {
    block_timestamp_type timestamp;
    account_name producer;
    uint16_t confirmed;
    block_id_type previous;
    checksum256_type transaction_mroot;
    checksum256_type action_mroot; // action的Merkle树根
    uint32_t schedule_version;
    optional<producer_schedule_type> new_producers;
    extensions_type header_extensions;
}

struct ICPBlockHeader {
    block_header header; // 区块头
    incremental_merkle blockroot_merkle; // 区块ID的Merkle树
    digest_type pending_schedule_hash; // 生产者集合的哈希
    signature_type producer_signature; // 本区块的生产者签名
}
```

ICPTx是跨链交易协议包，包含跨链交易的有效载荷数据，并包含到区块头的Merkle证明：

```
struct action {
    account_name account;
    action_name name;
    vector<permission_level> authorization;
    bytes data; // 跨链交易的载荷数据
}

struct action_receipt {
```

```
    account_name receiver;
    digest_type act_digest; // action的哈希
    uint64_t global_sequence;
    uint64_t recv_sequence;
    flat_map<account_name,uint64_t> auth_sequence;
    fc::unsigned_int code_sequence;
    fc::unsigned_int abi_sequence;
}

struct ICPTx {
    digest_type block_id; // action所在的区块头
    action_receipt action;
    vector<digest_type> action_merkle_proof; // action的Merkle证明
}
```

5.2 跨链合约

跨链合约同时部署在PCCS并行链和EOS主链上，合约账户名同为PCCSchaintoeos，处理双向的交易action，提供如下接口：

- postblock: 提交来源链的区块（头）
- posttx: 提交来源链的跨链交易
- call: 提交去往目标链的跨链交易

用户或应用调用call发起跨链交易，中继者监听到后调用postblock提交ICPBlockHeader，调用posttx提交ICPTx。前者是调用来源链跨链合约，后者是目标链跨链合约。

跨链最具代表性的应用是跨链资产转移，下面举例。

从EOS主链到PCCS并行链

1. Alice发送一笔10个EOS的交易给EOS主链的跨链合约，接收账户是Alice在PCCS并行链上的账户。

2. 中继者监听到了这笔资产转移交易，等待这笔交易所在的区块已被确认后，包装成跨链协议包，发送给PCCS上的跨链合约。

3. Alice在PCCS上的账户收到了10个CEOS代币（EOS在PCCS的表示法）。

4. Alice在PCCS上发送了4个CEOS代币给Bob。

5. Bob发送4个CEOS的交易到PCCS的跨链合约，接收账户是Bob在EOS主链上的账户。

6. 中继者监听到了这笔赎回交易，等待这笔交易所在的区块被确认后，包装成跨链协议包，发送给EOS主链上的跨链合约，跨链合约处理后将4个EOS释放给Bob。

以上流程结束后，Alice拥有6个CEOS，Bob拥有4个EOS。

类似的，从EOS C并行链到EOS主链，也是相似的流程。

5.3 跨链通道

跨链最基本的前提在于，能够验证B链收到的跨链协议包确实是A链产生的，并且与之相关的逻辑已经在A链上执行（比如资产转移时锁定一方资产），那么可以安全地在B链上执行后续的应用逻辑（比如产生另一方的等值资产）。我们设想了跨链通道这一抽象概念来保障这个基本前提。

5.3.1 开启通道

两条链建立跨链通道，必须基于某个信任种子，后续的证明都可追溯到这个信任种子。对于一条链来说，信任种子可以是另一条链的创世块或任何已确认的签名区块头。从A链信任种子开始，B链可以验证任何后续A链的区块头的有效性，并且必须验证签名的超级节点集合是否正确。EOS的超级节点集合是随着持续的投票进程而动态变化的，那么也得验证每一次节点的变动是否体现在区块头中。

EOS区块头中超级节点集合及其变动版本号：

```
struct block_header {
    ...
    uint32_t schedule_version;
    optional<producer_schedule_type> new_producers;
```

```
    ...
}
```

这保证了基于信任种子的持续验证的内在一致性和可审计性，但如果发生分叉攻击，那么就必须再次通过链上治理来校正。

5.3.2 通道运转

通道的持续运转，体现在一条链跟随另一条链的区块头一直前进，也即从区块头H_g到区块头H_h，其中h > g。如果不要求h = n + 1，则意味着不需要区块头的连续跟随。BFT-DPOS共识机制下，只要被考察的两个区块头所代表的区段内，超级节点集合的变动少于三分之一，则能保证跟随的安全性。

5.3.3 关闭通道

两条链之间的跨链通道，正常情况下永远不应该关闭。但在遇到不可解决的极端情境下（比如拜占庭错误），可以通过链上治理或另一条链上的超级节点的签名集来关闭通道。这时，需要保障用户资产的重新赎回。

5.4 中继者

加持了跨链合约的EOS区块链，自身可以表达和记录跨链的意图，但不能也不会主动发起跨链通信，只能被动接受外部调用其跨链合约的接口。我们将实现中继者，作为EOSIO软件的插件，可同时部署在PCCS并行链全节点和EOS主链全节点中。中继者负责在EOS和PCCS链间实时双向同步ICP包。

5.4.1 中继算法

```
while true
    set pending = tail(outgoing_A)
    set received = tail(incoming_B)
    if pending > received
        set U_h = A.latestHeader # 获取A链的最新区块头
```

```
if U_h != B.knownHeaderA
    B.updateHeader(U_h) # B链同步A链的最新区块头
for i from received to pending # 遍历未处理的ICP包
    set P = outgoing_A[i] # 获取ICP中的载荷数据
    set M_kvh = A.prove(U_h, P) # 获取A链的Merkle证明
    B.receive(P, M_kvh) # 发送交易给B链，触发合约动作
```

中继最新区块头，相比于发送跨链交易，开销大得多。因此中继者可以等待足够多的未处理ICP包，然后一次性处理，这样相当于多笔跨链交易对应一次区块头同步。这将大大减少目标链上的计算开销，但也带来了跨链交易的延迟，中继者可以根据实际情况折中动态调整。

我们设计中继过程是完全异步的、无需实时的、幂等的，却必须保证有序、可证明、超时可控。因此采用上文所述的跨链消息队列，在链上缓存跨链交易协议包。消息队列的数据结构内建在跨链合约中，队列中元素存储于区块链状态数据库。

5.4.2 系统参数定制

- 每个PCCS最多只能投票3个超级节点，而不是30个
- 投票用户参与节点奖励分红，由宪法规定分红比例

5.4.3 系统插件

- kafka插件

内置插件Kafka生产者客户端功能到链节点。流实时细节结构的块/事务/动作数据，反映了区块链到Kafka集群的所有状态转换。任何消费者都可以使用这些数据进行各种业务逻辑处理，保证了即时性或不可逆性。基于它的原语，任何人都可以实现block explorer、分散钱包和更多样化的DAPPs。

- MySQL插件

Mysql 作为著名的关系型数据库，历史悠久、性能卓越服务稳定软件体积小，安装使用简单，并且易于维护，安装及维护成本低等优点被其大量企业作

为数据库首选，因此我们也集成了mysql数据库插件，PCCS数据持久化存储为各类型用户提供多种数据持久化方式，mysql插件配置简单使用方便，此功能将满足各类用户区块链数据差异化使用需求。

• 投票分红

自EOS主网上线以来，EOS投票率过低，分析其原因为何普通用户没有参与投票动力，区块链系统都会有token经济，所谓token经济就是通过经济激励手段内置到区块链系统吸引更多用户加入进而促进系统发展，因此我们希望通过投票分红手段刺激用户投票热情，让更多的普通用户来参与PCCS发展，只有让普通用户加入、让更多人参与进来分享和参与整个网络的发展红利才是更好的区块链系统，通过投票分红能带来更多的系统反馈，让我们听到不同系统角色的声音，能进一步促进系统社区化治理形成，PCCS将会让投票用户参与到社区治理中来。

• 最低资源保障计划

EOS主网上的一个隐形问题，即有的用户拥有了EOS账户，账户中存在余额，但是资源缺乏（RAM，CPU，NET）无法进行交易。这是由于EOS交易需要消耗资源，而该资源需本身又需要用户进行购买或抵押，而购买或者抵押也是属于交易，这就陷入了死循环。当然我们可以在的创建账户的时候就配置一定的资源，但这又增加了用户的使用成本，体验性变差。

为了解决这个问题，PCCS在EOS的基础上，增加了最低资源保障机制，该机制默认分配给每个用户免费的资源额度，并修改了系统合约，添加了可配最低资源功能。这样用户的基本链上操作需求都能被满足，对于更多使用需求的用户，超出最低额度的资源使用仍然需要进行抵押。

5.4.4 系统合约

- Token合约：支持由跨链合约内联调用注册新的Token
- CrowdSale众筹合约：支持调用Token合约
- NameAuction名字竞价合约：顶级名字和次级名字的竞价

5.4.5 协同治理

PCCS尊重EOS主链的宪法，但也拥有自己的宪法。当EOS社区进行宪法修正提案投票时，如果最后实施的链上变更将影响PCCS与EOS的互操作，PCCS应当同时发起与之适配的宪法修正提案，并在恰当的时刻将适配变更同步实施到PCCS并行链上。考虑最坏情况下，PCCS宪法与EOS宪法的同步修订不能取得社区的一致性意见，后果将是跨链不能正常工作，那么预计很大一部分社区成员是同时持有两个链的原生Token，为了保障自己的利益，将会努力促成跨链功能的恢复，因而在宪法修订上最终将达成共识。

PCCS链上治理，将采取有别于EOS主链的提案投票方式：

1. 全网PCCS持有者投反对票，如果一月内投票数超过总数的三分之二，提案不通过;

2. 超级节点投赞成票，如果一月内超过总数的三分之二，提案通过；

3. 超级节点投赞成票，如果一月内不超过总数的三分之二， 提案不通过

链上治理的结果很多时候将影响PCCS的系统机制，涉及到每一个PCCS持有者的权益。第一阶段给予全网PCCS持有者投反对票的权力，是为了既避免超级节点联盟或合谋的中心化危害，又调动PCCS持有者参与链上治理的积极性。但全网投票，很难达到总数的三分之二，这也表明社区的反对意见不足以直接推翻提案，所以第二阶段继续由超级节点投票，加速提案表决。

六、应用场景

6.1 同构跨链群

区块链世界不可能由一条区块链主导，将来的形势一定是多种应用场景DAPP的并存、多链并存。如果使用EOS主链来承载所有业务，除了成本昂贵，还非常不利于商业应用对接。EOS“主链+并行链”多链并行模式的扩展性架构，分离了主链和并行链，由不同的并行链来承载各类商业应用，极大地降低部署成本，满足百万级TPS需求。并行链可随业务复杂度继续平行扩展，承载事务数指数级上升。PCCS将作为并行链基础设施解决方案，与社区成员、机构、企业一起构建EOS同构跨链群。

6.2 连接PCCS异构跨链体系

我们相信未来的区块链不仅在去中心化社区中具有广阔的商业落地前景，千万中小企业同样需要区块链作为价值传递和无需信任的共识达成的基础服务。并且无论是公有链、联盟链还是企业内部的私有链，都需要对接到一个公有网络以实现更大范围的互联互通。

PCCS-chain异构跨链体系，将作为一个更大的生态项目被推出。PCCS并行链将成为第一条纳入PCCS-chain异构跨链体系的公链，作为连接EOS跨链群与其他区块链的纽带。

6.3 PCCS Chain 隐私特性

随着区块链技术的应用和发展，PCCS在未来的blockchain生态中将优先升级交易的隐私特性，创建一个具有合规性的、真正的数字资产的价值转移生态系统。对比现金交易，使用者可以选择是否为每笔交易留下书面记录。这样，未来我们将共同创造一个个人和企业都可以使用的货币体系。

纵观比特币的10年发展历程，大家对于隐私性的交易非常重视，并且越来越多的人都会意识到金融隐私的必要性，比特币社区也将不得不采取行动。在我看来，没有隐私就很难保证数字黄金的地位。总量恒定的模式的确更有可能保值，而非成为交换媒介。

PCCS Chian 已经初步进行了隐私特性需求的研究和验证，将在下一步的开发过程中根据技术布局逐步完成，使用户在使用的过程中真正体验到自己的隐私自己来管理。并且逐步融合隐私数据的确权、授权、交易等行为需求，结合AI深度学习，帮助PCCS生态的高新科技DAPP落地和发展。

6.4 PCCS Chain 匿名性

从比特币的发起人中本聪开始，就对区块链的匿名性就做了重要的阐释，在区块链发展早期，更有很多技术人员尝试通过混币技术和环签技术让交易混乱以提升比特交易记账的匿名性，然而这两种方法都出现了问题。对于混币器，依赖于一个可见的混币地址并要求你完全信任这个混币器。混币技术同时还会受到交易图表分析的影响，通过交易图表分析能识别混币服务并标记出那些可疑的Token。

与 Bitcoin 相比，Zcash 集成了一种机制在转账自动隐藏发送方、接收方的地址，甚至转账金额。仅限定持有浏览权限秘钥的人员查看。与隐私匿名技术混币 Dash、环签名 Monero 相比，Zcash 可达成任意等级强隐私保护。

对比研究MimbleWimble、混币、环签名、零币协议及其他方案，PCCS做了更深层级的试验，为保护使用者的身份信息以及交易信息，我们将对链上用户交易信息进行加密隐藏，自动隐藏区块链上所有交易的发送者、接受者及数额。只有那些拥有查看秘钥的人才能看到交易的内容。用户拥有完全的控制权，他们可自行选择向其他人提供查看秘钥。另外为用户提供安全的支付通道，同时使用公有区块链来维护一个去中心化网络。通过使用新的协议技术实现解决匿名交易问题。

PCCS 在隐私保护以及匿名性上做了非常充分的准备，并计划在未来的支付场景中有更多的可扩展的技术支持，给使用者和企业提供高效的、安全的、零手续费的开放网络，同时还能保证交易的隐私性。

6.5 PCCS Chain 钱包

PCCS钱包是一个跨链多币种钱包，将作为EOS同构跨链群的生态入口。未来PCCS钱包将继续支持异构跨链体系，作为多链互联的资产管理和应用平台入口。

6.6 分布式交易所

随着数字资产的规模和种类不断增加，各类代币间的交易需求水涨船高。伴随着数以千计的新代币的出现，以及传统资产的代币化，交易需求又被进一步放大。当前市面上的交易所大部分都是中心化的，主要优势在于效率和方便，但同时面临以下三大问题：

- 缺乏安全性：中心化的交易所用户常常都是把自己的私钥（资产）交给一个中心化的实体来管理，这使得交易所很容易成为黑客攻击的对象，数字资产的交易本身对安全性要求非常高，能做到满足安全性能要求的交易所也很少。
- 缺乏透明性：交易所占据着大量用户资产，在监管缺失的环境中，利用暗箱操作手段攫取用户利益屡见不鲜，同时中心化交易所还面临着不确定的政策监管问题。

• 缺乏流动性：中心化交易所之间的订单需求无法共享，难以提供充分的流动性和交易深度。这不但会影响用户体验，还会大大增加用户的交易成本。

因此，无需信任的代币（资产）交易自然成为了区块链技术一个令人期待的使用场景。PCCS作为一条可以与EOS主网进行跨链资产转移的平行链，可以较容易地实现高效、安全的去中心化交易所。

6.7 跨链DAPP

目前除了数字货币本身，DAPP世界缺乏杀手级应用。大多数DAPP受区块链性能的影响，并没有给用户一个很好的使用体验。PCCS并行链及其ICP协议，可以帮助大型DAPP跨链部署，无缝横向扩展和价值流转，既可以带来匹敌传统互联网应用的用户体验，又能够充分发挥区块链价值互联网的优势。

七、分配方式

PCCS初始发行量8400万枚，分配方式如下：

40%基金会持有，用于PCCS主网运营；

30%用于生态激励，向PCCS的跨链交易及应用开发提供奖励，其中包括跨链交易补贴；

20%用于节点扶持激励，分期为开发者社区提供激励；

5%用于市场推广，赏金社区及空投活动；

5%用于交易所对接及必要的流动性管理。

八、PCCS发展路线规划

• 第一阶段（2019.08）

持续迭代开发PCCS项目启动

• 第二阶段（2019.09~2019.12）

完成中继、跨链合约等主要组件研发

• 第三阶段（2020.01~2020.06）

跨链调试及PCCS测试网搭建，进行安全性验证和上线测试网络，进行安全性检查和测试。

• 第四阶段（2020.07~2020.12）

PCCS主网启动及生态建设，完善技术开发文档，定制PCCS主要的系统参数，开发必要的系统插件，完善PCCS跨链功能，开发钱包、区块链浏览器等，并上线PCCS主网。

• 第五阶段（2021.01~2021.10）

PCCS匿名隐私技术研发。

PCCS匿名支付研发。

PCCS匿名智能合约平台研发。

PCCS跨链应用模型研发，统一同构跨链模型，建设EOS同构跨链群。

• 第六阶段（2021.11~ ）

PCCS异构链功能研发，开发和构建PCCS-Chain异构跨链体系，帮助PCCS连接主流异构公链。

8.1 相关资料

8.1.1 Cosmos

Cosmos是构建PCCS并行链的最初想法来源，它是第一个将异构跨链技术系统化并在代码上付诸卓有成效的实现的公链项目。其采用Tendermint 共识底层，通过ABCI进行上层模块开发，提出Hub和Zone等清晰一致的跨链模型，并

实现了一个连接以太坊的Peggy Zone的原型。然而，Cosmos从始至终都将以太坊作为跨链的首要目标，无暇参与贡献EOS生态。并且Cosmos选择了模块化机制来进行功能扩展，目前没有内建智能合约虚拟机的计划。

8.1.2 以太坊分片

以太坊分片技术，是解决区块链扩展性的另一种新颖方法。以太坊基金会和社区在这项技术上的探索已经很久，但需要硬分叉以太坊，且落地日期依然遥遥无期。而PCCS务实地选用多链并行和跨链协议的方式来达成横向扩展，对EOS主链没有侵入性，且实现上安全可靠。

8.1.3 Polkadot

Polkadot是另一种解决异构跨链难题的公链项目，它设计了4种角色（收集人、钓鱼人、提名人、验证人）和2种链（中继链、平行链，类似于Cosmos的Hub和Zone），且对中继链的验证人进行分组，每个组中的验证人必须同时参与对应的平行链的验证。这带来了很高的复杂度和耦合性，平行链的独立性受到很大制约。

8.1.4 Zcash

Zcash 是一种加密货币，使用加密技术为其用户提供比其他数字货币（如比特币）更强的隐私。最初是由一个命名为 Zerocoin的协议发展而来，随后其团队开发了 Zerocash 系统，直到2016年将其发展为 Zcash 加密货币。

8.1.5 Monero

Monero 创建于2014年4月，与 Zcash 不同的是它并没有选择基于之前的区块链系统开发，并从底层实现有着很好的模块化设计，因此具有比较好的扩展性。

Monero 的特点在于 首先它虽然也采 用了了工作量证明（POW）的共识机制，但是与之前的许多加密货币不同，Monero 工作量证明算法CryptoNight是

为AES密集型和很耗内存的操作，这显著降低了GPU对CPU的优势，换句话说降低了了工作量证明算力集中化的风险。

8.1.6 Dash

Dash是第一个以保护隐私为目的设计的数字货币，它采用的中心化混币方案的本质是单纯地将一笔资金在多个地址中进行多次转移，实现简单，易于操作，混币过程不需要其他的技术支持。中心化混币方案在各类数字货币系统中具有极高的适用性，但是，现有的方案要求参与混币的人员在线进行混币。如果双方就混币的数额不能达成一致的话则必须推迟，为了使得混合充分，交易易普遍存在时延问题并且混币器是中心化部署的，混币器节点能获取交易的所有信息，能盗币。中心化混币方案的大多数改进方案是通过增加第三方违规的代价来防止盗窃和信息泄露的发生，不能从根本上杜绝违规行为的发生；采用盲签名等密码学技术的混币方案会增加计算代价，并且由第三方执行混币过程必然会带来额外的服务开销。

总结

PCCS秉承构建区块链互通互联的使命，打造跨链支付网络体系，同时致力于区块链隐私保护，繁荣区块链生态，推动人类经济和社会体系结构的发展和进步。

引用

- Bitcoin: https://bitcoin.org/bitcoin.pdf
- Ethereum: https://github.com/ethereum/wiki/wiki/White-Paper
- Zerocash: http://zerocash-project.org/paper
- Monero: https://getmonero.org/
- EOS: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md
- Block.one: https://block.one/
- JIT: https://en.wikipedia.org/wiki/Just-in-time_compilation
- Merkle Tree: https://en.wikipedia.org/wiki/Merkle_tree
- Message Queue: https://en.wikipedia.org/wiki/Message_queue

• Cosmos: https://cosmos.network/docs/resources/whitepaper.html
• Polkadot: https://polkadot.network/Polkadot-lightpaper.pdf
• Filecoin: https://filecoin.io/filecoin.pdf
• BFT: https://en.wikipedia.org/wiki/Byzantine_fault_tolerance
• Tendermint: https://tendermint.com/docs/