ORIGINAL COMM CIMELIA

— OCC —

乾元通宝

目录

一 前言

- 万物来自于虚空,现实中的花花世界,在电脑里都可以呈现,如梦如幻。
- 而电脑的程序其实只是1和0的变化而已,这就是所谓的”二进制”。实际上，现实的生活也是1和0的变化，这个学问在古老的《易经》里已经阐明，就是阴和阳。区块链不过是程序的一种，实际上也是1和0的变化，也是阴和阳的变化。一阴一阳之谓道，就变化出现实的五彩缤纷。
- 今天，太极链横空出世，“太极者，本无极也”，这是古人说的话，大概是说最根本的东西，可能是空的，和没有差不多，就像这个宇宙，只是由一个奇点的爆炸而来，据说宇宙所有物质的核子的质量，加起来其实很小很小，几乎是没有；
- 那么区块链呢？其实是一个看不见也摸不着的东西，当我们去使用它时，它确然存在，当你想拿出一个东西来给人看时，其实你根本拿不出来，它只是电脑程序的一增一减（一阴一阳）的变化而已。
- 空有双融，有无相生，这或许就是宇宙的真相。
- 所以，我们取名太极链。

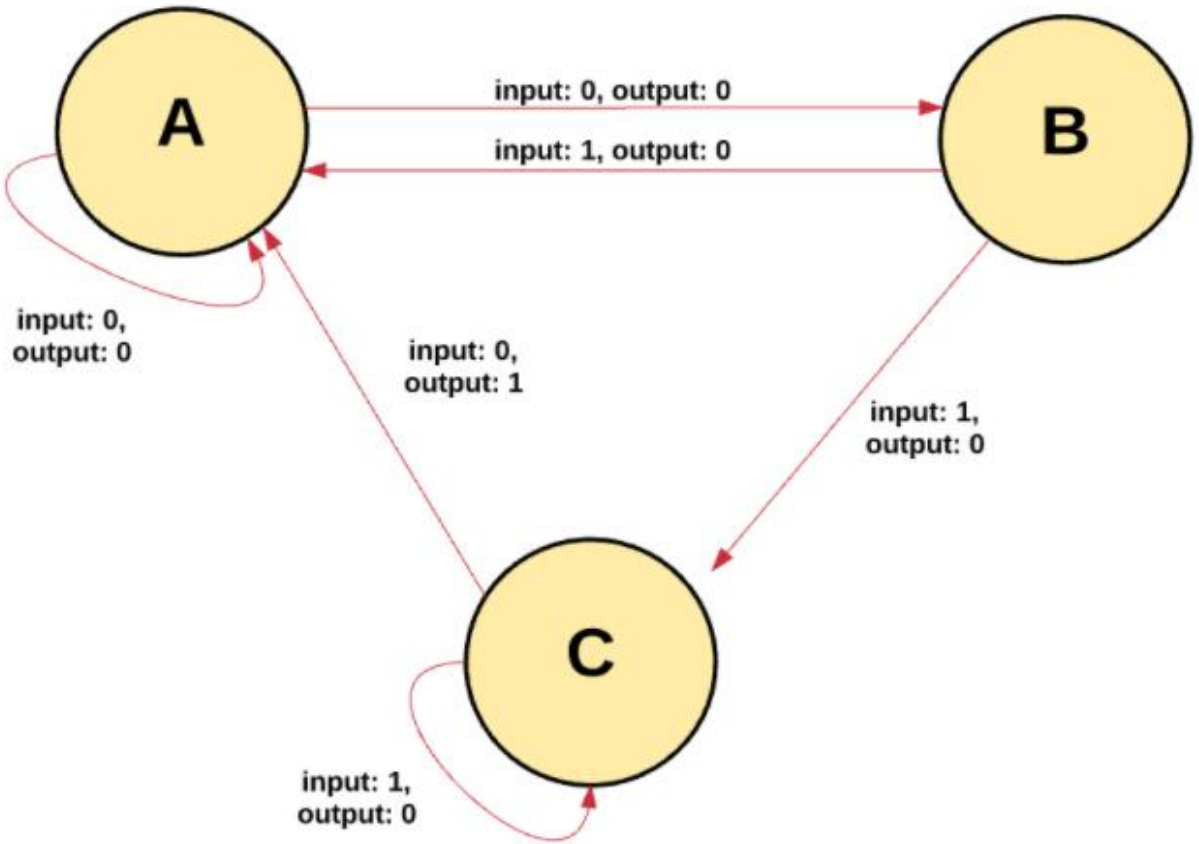
二 科技的目的

- 在本文正式开始之前，我们要谈一个话题：科技的目的。因为区块链目前是令很多人痴狂的领域，说其“痴”，是因为据大家所透露：目前很多在做所谓区块链工作的人，其实不太懂区块链，但是这“很多的人”都在痴痴地迷着区块链，有点着魔的味道。经过仔细思考，我们看到这可能基于两个原因，一个是区块链确实技术上比较难懂，越难懂，大家就越想弄懂；另一个原因是比特币带来的“赚钱示范效应”。同时，区块链也确实会是人类科技发展的一个方向，随着区块链的普及和发展，将在很大的程度上改变企业的运行规则乃至社会的某些运行规则；这样也会以区块链为中心，形成庞大的产业，不仅影响到我们的生活，也会改变目前的财富格局甚至社会格局。
- 人类文明的产生是来自于追求宇宙的真理,所谓“求道”,就是这个意思。等而下之，有所谓“思想”，而很多伟大的改变，首先来自于思想的改变，因为思想的改变，才会产生推动事物变化的力量，通过人类的智慧行动来创造现实生活的财富。
- 思想引领技术，但反过来，技术也深深地影响着思想，所以有所谓“区块主义”的出现，甚至认为，通过区块链，那些哲学家所向往的理想社会，甚至乌托邦类的理想国，均可以实现，因为区块链是完全节点化的，大家完全平等，自由，共享，自治。

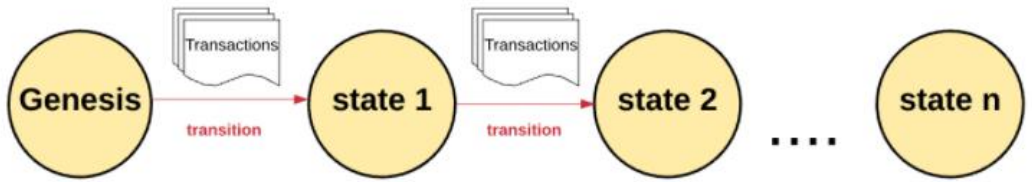
- 其实，人类的发展，依据欧洲发展史来看，大约是经过了这么一个过程：人类由原始思想而形成宗教文化，复由于对宗教的反动，而有哲学思想和科学实验的产生，哲学是依据思想理论来推断人生和宇宙，科学则系从研究实验来证明宇宙和人生。
- 自欧洲文艺复兴运动以后，科学支配着这个世界，形成成以工商业为最中心的物质文明。一般从表面看来，科学领导文明的进步，惟我独尊，宗教和哲学，将无存在的价值。事实上，科学并非万能，物质文明的进步，并不就是文化的升华。于是在这科学飞跃进步的世界中，精神文化仍有其不容忽视的价值。
- 我们今日深入区块链领域的学习和探究，乃至应用，不可忘记“文化这个根本”，尤其当区块链与金融结合在一起时，在很大程度上“将改变金融的格局”，但是，请别忘记了，那些有能力改变这个格局的，或者参与到这个格局的变化中的人们，科技的目的，其实也不过是为人类的“心安”而服务的，是为了更美好的人类的未来，而不是可以肆意妄为的。
- 所以，太极链的重点，是用东方文化的理念，来打造一个“文化的家园”，这是一个不冠以“文化”之名的“文化之链”，古人云“文以载道”，今日，我们也要提倡“科技载道”，或者可称为“术以载道”吧！

三 区块链

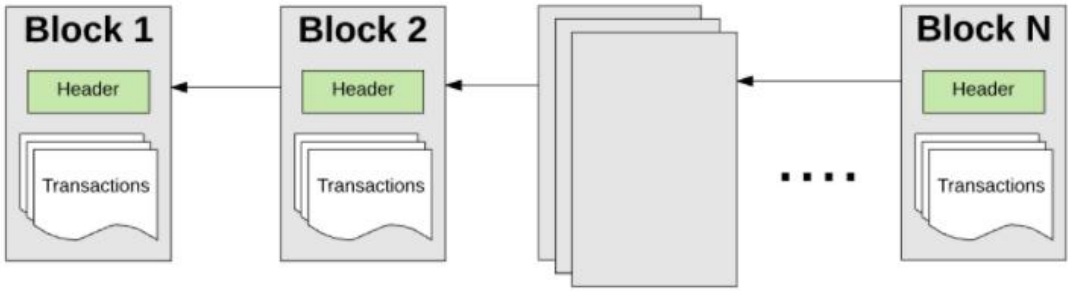
- 中本聪研发比特币，带给了世界革命性的俩个变革：一个是点对点的电子货币，无需担保，无需信任，却维持着不可思议的价值，这给货币演变提供了历史性的发展方向；另一个是基于交易顺序而达成共识的“区块链”。
- 本质上,比特币区块链其实就是一个具有共享状态的密码性安全交易的单机(cryptographically secure transactional singleton machine with shared-state).
- 这段话包含三个要义:
- （1）“密码性安全(Cryptographically secure)”,这是指用一个很难被解开的复杂数学机制算法来保证这个区块链运营的安全性。可将其想像成一个超级防火墙。这就使得欺骗系统是几乎不可能的（比如：构造一笔假的交易，消除一笔交易等等）。
- （2）“交易的单机(Transactional singleton machine)”,这是说若为系统中产生的交易负责任,类似只有一个权威的机器实例,没有第二个。换句话说，只有一个全球真相是大家所相信的。
- （3）“具有共享状态(With shared-state)”,这是指在这台机器上存储的状态是共享的，对每个人都是开放的。所以区块链的本质就是一个基于交易的状态机(transaction-based state machine),如图:


A
B
C
input: 0, output: 0
input: 1, output: 0
input: 0,
output: 0
input: 0,
output: 1
input: 1,
output: 0
input: 1,
output: 0

- 在创世纪状态(genesis state),类似于此时是一块空白的白板，网络中尚无任何交易。当交易被执行后，这个创世纪状态就会转变成最终状态。而且在任何时刻，这个最终状态都代表着区块链当前的状态,如图 :



- 通过共识机制，,这些交易都被“简化的方式组团记录”到一个区块中。一个区块包含了一系列的交易，每个区块都与它的前一个区块链接起来。如图:



- 因为中本聪的这个伟大的发明，21世纪在某种程度上很可能会是区块链大发展的世纪，比特币的诞生也标志着一个新时代的到来。
- 区块链的特性，给了后来的开发者无穷的想像，也给了大家发展的方向；区块链诞生于“一种点对点的电子货币的构想”，但是却可以在很多领域发挥其绝佳的功用；
- 时至今日，区块链主链的开发已经蓬勃发展了，其中不乏非常具有技术创新的作品，可以预见，在不仅的将来，可能会出现“万链竞发”的局面。

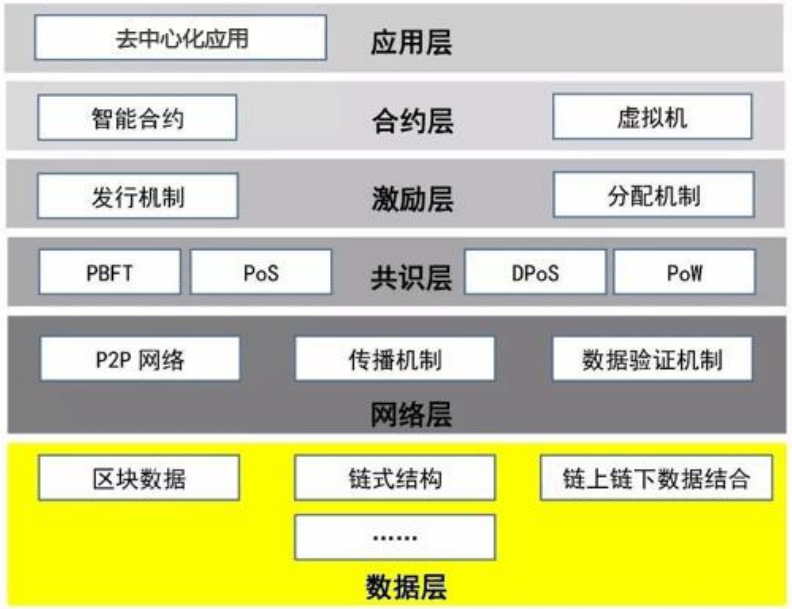
四 太极链

- （一）概要
- 1 以太坊通过详细地研究比特币及其区块链特性，在扩展性和实用性上努力进行提升，它所提供的区块链是一种内置的完全成熟的图灵完备的编程语言，可用于创建编码任意状态转换功能的“智能合约”，允许用户创建上述任何系统，还有其他许多我们可能还没有设想到但是仅仅通过在几行代码中编写逻辑就可以实现的功能。
- 太极链公链的创建，就是在详细研究比特币，以太坊的基础上，用以太坊最新源码为基线版本，做了适当的优化以支持太极链的目标和愿景，主要的修改包括创世区块参数、预挖币总量、奖励规则、出块速度、共识算法等。
- 所以，太极链具备以太坊所有的功能，并且，在很多方面，优化了相关功能，同时，太极链将会以“华语圈”普通人也看得懂的方式面世。
- 2 围绕着太极链主链，有大量辅助性的工作需要去完成：
- （1）太极链周边配套软件，包括区块浏览器、移动端钱包APP、OCC币和代币交易系统等；
- （2）第三方应用系统接入API接口和SDK开发包等，方便开发人员基于太极链开发基于区块链的去中心化应用；
- （3）智能合约编辑、编译和部署工具，提供常用合约代码模板，实现非专业人士也可以编写和部署智能合约。

- （二）规划
- 1. 规划1.0版本　　在8月20号前推出1.0版本，这个版本具有如下功能：
- （1）太极链公链上线，公链完全开放，任何人和组织均可以通过太极链软件接入太极区块链网络，搭建自己的区块链节点，在节点上进行挖矿或者开发区块链应用。
- （2）太极链区块浏览器，支持实时呈现区块生成信息、区块信息查询、交易信息查询等。
- （3）太极链钱包APP软件，同时支持Android和ISO（IOS版本将在2.0版本推出）两种系统，功能上支持太极链本币OCC和各种基于太极链的代币的交易。
- （4）太极链官方网站，网站介绍太极链的：
- （4.1）ERC20标准代币发行功能，支持在太极链网页版上快速部署代币合约，用户无需掌握区块链和智能合约编程语言，即可快速完成合约的部；
- （4.2）2.0版本时在太极链钱包APP上快速部署代币合约；
- （4.3）太极链交易所系统，支持OCC币和太极链上各种代币的交易。

- 2. 规划2.0版本
- （1）开放太极链API接口，支持第三方应用接入太极链，方便开发人员开发OCC币和代币的交易，以及基于太极区块链的各种去中心化应用。
- （2）增强太极链区块链浏览器的能力，包括支持账户历史交易记录查询、智能合约源码浏览、代币信息浏览等。
- 3. 规划3.0版本
- （1）优化太极链的共识算法，缩短交易确认时间，以支持大规模的交易的需求。
- （2）提供通用智能合约代码的部署，在太极链钱包APP和区块链浏览器集成智能合约编辑和编译软件，并提供部署功能。以支持金融、供应链、文化娱乐、智能制造、社会公益和教育就业等典型应用场景。
- （3）太极钱包APP整合交易所部分功能，例如交易和价格走势等。
- （4）《易经》告诉我们关于“易”的学问：易者，变易，简易，不易，通称三易，其中“简易”之道，太极链的研发人员至为欣赏，所以，在太极链上将来布署“智能合约”一切从简，或者操作手法与以太坊类同，所不同之处在于，太极链更适合华语圈的人使用，这样将大大普及华语圈的区块链应用！

- （三）太极链技术部分
- 1. 太极链区块链平台架构
- 系统架构决定了应用的适用范围、跨链及链上链下的数据整合的可行性，甚至商业变革的方向。因此平台架构的升级理念，无不体现平台对于区块链技术和商业模式的理解。太极区块链的架构分为数据层、网络层、共识层、激励层、合约层和应用层。如图：



- 2. 数据层
- 数据层是最底层的技术，封装了底层区块数据的链式结构，以及数字签名、哈希函数和非对称加密技术等多种密码学算法和技术。主要实现了数据存储、账户和交易的实现与安全两个功能。上述技术都已经在计算机领域应用多年，是相对成熟的技术。
- 3. 网络层
- 网络包括P2P网络机制、数据传播机制和数据验证机制等，主要实现网络几点的连接和通讯。P2P组网技术早先应用于BT类的P2P下载软件中，是一种很成熟的技术。
- 4. 共识层
- 共识层主要封装网络节点的各类共识机制算法，实现全网所有节点对交易和数据达成一致，防范拜占庭攻击、女巫攻击和51%攻击等共识攻击，其算法称为共识机制。比较常见的共识算法有工作量证明机制（PoW）、权益证明机制（PoS）、拜占庭容错算法（BTF）等。太极链采用工作量证明算法。

- 5. 激励层
- 激励层主要实现区块链代币的发行和分配机制，该层主要出现在公有链中，用以激励遵守规则参与记账的节点，惩罚不遵守规则的节点，促使整个系统朝着良性循环的方向发展。
- 6. 合约层
- 合约层主要封装各类脚本、算法和智能合约，赋予账本可编程的特性。太极链通过虚拟机的方式运行代码，实现智能合约的功能。
- 7. 应用层
- 应用层封装了区块链的各种应用场景和案例，在太极链上的各类去中心化应用（DAPP）。

- （四）区块链平台核心技术组件
- **1. 共识机制**
- 共识机制是区块链系统中各个节点达成一致的策略和方法。目前主流的共识机制有PoW（工作量证明机制）、PoS（权益证明机制）、DPoS（委托授权的权益证明机制）、Raft、PBFT（实用拜占庭容错算法）等，以下是各个主流共识机制的对比分析：

	PoW	PoS	DPoS	Raft	PBFT
场景	公有链	公有链、联盟链	公有链、联盟链	联盟链	联盟链
去中心化程度	完全	完全	完全	半中心化	半中心化
记账节点	全网	全网	选出若干代表	选出一个leader	动态确定
响应时间	10分钟	1分钟	3秒左右	秒级	秒级
存储效率	全账本	全账本	全账本	全账本	全账本+部分账本
吞吐量	约7TPS		约300TPS或更高		约1000TPS或更高
容错	50%	50%	50%	50%	33%

- 2. 通信/P2P技术
- 太极链通常采用P2P技术来组织各个网络节点，每个节点通过多播实现路由、新节点识别和数据传播等功能。在通信/P2P技术方面，太极链客户端P2P协议是一个标准的加密货币协议，能够容易地为其他加密货币实用，仅有的改动是引入了“幽灵协议”。
- 3. 存储
- 要实现分布式账本的大规模应用，存储的开销是需要解决的关键问题之一。区块的数据结构通常只能追加记录而不能删除或者修改，以能够使新加入的节点对全网的完整交易历史进行验证，随着历史数据的增长，存储开销成了影响区块链系统扩展性的一大问题。太极链与比特币一样，使用Merkle树存放交易散列，在面临不断增长的数据时，一旦需要回收硬盘空间，可以选择将老旧的交易从Merkle树种删除。
- 除此之外，太极链还采用了状态快照的方式来节约硬盘空间，即区块头除记录当前区块所有交易的根散列外，还记录当前区块及过去所有区块中的状态根散列。
- 所以，如需节约空间，节点可以清空状态快照之前的交易历史，值保留最新区块和完整的信息状态，但这样相当于在安全性和去中心化上作出了一定的妥协，因为全量历史记录有可能回退到云化甚至中心化存储。

- 4. 计算效率
- 若交易可以被并行验证，则可以通过简单地增加CPU数量来提高吞吐量。但若具备状态持久化能力的智能合约是顺序相关的，则难以并发验证。太极链的交易理想中可以通过区分解决智能合约状态持久化问题，从而使得交易可以被并行验证（即将各个合约分到不同的逻辑区中，每个区中的合约都顺序执行，而不同的区之间并行执行），但该功能尚未实现。
- 5. 数据结构
- 在区块链技术中，数据以区块的方式永久存储。区块按时间顺序逐个先后生成并连接成链，每个区块记录了创建期间发生的所有交易信息。区块的数据结构一般分为区块头（Header）和区块体（Body）。其中，区块头用于链接到前一个区块并且通过时间戳特性保证历史数据的完整性；区块体则包含了经过验证的、区块创建过程中产生的所有交易信息。太极链的区块头中除了前一个区块的引用信息、区块号、交易信息的Merkle树的根哈希值。

- （五）区块链平台应用功能
- 应用功能是指区块链平台为进行用户身份管理、实现上层应用所需的基础功能组件，应用功能是在核心技术组件基础上，提供了针对区块链应用场景的基础管理功能，一方面其允许通过使用智能合约的方式制定商业规则以管理交易，灵活操作链上资产，并辅以账户体系使区块链生态与现实商业社会更加紧密地衔接；另一方面，对于联盟链和专有链，通过应用功能中的身份认证、私钥保护等手段，强化成员管理，实现可信交易和防伪朔源。同时，通过设置节点权限，与现有商业规则中的监督体系保持一致。
- 1. 身份认证
- 太极链采取匿名身份认证体系，对线上线下的身份匹配无强制要求。
- 2. 账户设计
- 太极链采用了余额账户机制。由于太极链是以智能合约为主要功能，而智能合约中要处理UTXO的状态相当困难，相比之下，余额设计更便于程序实现。

3. 私钥保护

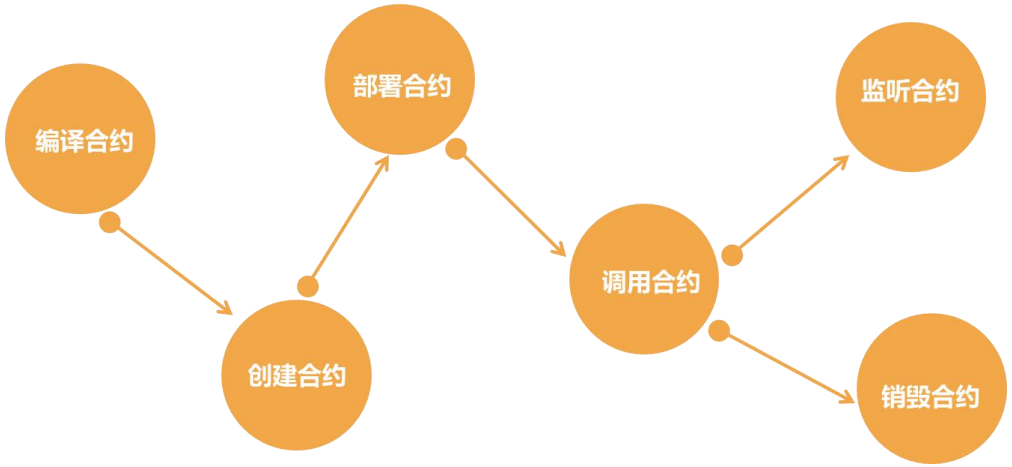
- 太极链采取的模式为：无人操作的挖矿/记账节点上不存储私钥，随同这些节点部署的智能合约也不使用私钥，所有的私钥部署于“端”，由用户本地存储。
- 4. 支持智能合约
- 太极链可实现“图灵完备（一切可计算的问题都能计算，程序逻辑自洽）”的智能合约功能，采用合约和共识相连。主要运用Solidity合约开发语言，具备图灵完备的特性。
- 5. 监管相关功能
- 太极链因其有公有链特征，监管可随时接入，但由于身份匿名性，监管接入的意义不大。
- 6. 特权机制
- 目前，特权机制主要有两类：一是暂停、回滚或者取消交易；二是改正数据。太极链不支持特权机制，一旦发生异常，无法通过特权机制进行回滚、取消交易或改正数据的处理。

- （六）太极链平台技术能力
- 1. 吞吐量
- 目前，太极链网络受限于CPU单线程性能。网络已达到每秒25次交易（在某种优化条件下），通过优化可能会提高到50TPS或100TPS。
- 2. 确认时间
- 当前太极链协议取决于节点根据在计算上开销更高的工作量证明（PoW）算法选择用于最长链的下一个区块。这种方法区块链每12秒左右提交一个新的区块，确认时间也是在12秒左右。
- 3. 可用性
- 太极链采用的工作量证明机制（PoW）提供了较高的灵活性和可用性。因为每个节点都独立构造区块而不需要其他节点的参与，节点可以随时加入或者退出网络，即使全网只剩一个节点，网络还是可以继续工作，但相应地它也失去了交易的最终性（保证交易不可撤销）。

- （七）太极链平台安全机制
- 区块链在设计中采用了分布式数据存储、共识机制、数字签名、加密算法等多种安全手段和技术。这些技术保证了数据的完整性、不可篡改性和一致性，从而保证了数据从交易、共识计算、区块确认、数据存储等全生命周期的安全性。随着区块链技术受到的关注日益增强、各类数字货币的价值飞涨，导致越来越多的不法分子渴望挑战区块链的安全性。例如，51%的攻击随着矿池的兴起而逐渐具备实现的可能性；区块链交易平台遭受攻击的事件频频发生。不过大部分的漏洞在于集中化的交易应用平台，而非底层技术平台的安全能力。下面研究将探讨区块链技术中各种安全机制的属性和特征，分析研究范围内平台在解决使用安全性、系统安全性、算法安全性、协议安全性等诸多挑战时所采取的策略。

- 1. 密钥生成机制
- 在用户账户密钥层面，太极链利用非对称加密算法生成公私钥。太极链的密钥生成机制为：随机数发生器生成私钥，再经过一种椭圆曲线算法SECP256K1生成公钥。
- 2. 密钥存储
- 太极链密钥生成后作为文件或字符串保存在用户终端或者托管到服务器，密钥文件是一个JSON格式的文本文件。
- 3. 密钥使用和密钥找回
- 太极链无定期更换机制，且私钥丢失后无法找回。
- 4. 防“双花”
- “双花”即二重支付，指攻击者几乎将同一笔钱用于不同交易。太极链的防“双花”采用了余额机制：每个账户都有一个状态，状态中记录了账户当前的余额，转账的逻辑即从一个账户中减去转账的金额，并在另一个账户中加上响应的金额，减去的部分和加上的部分必须相等。

- （八）智能合约
- 1. 什么是智能合约
- 太极链上的程序称之为智能合约， 它是代码和数据(状态)的集合。智能合约可以理解为在区块链上可以自动执行的（由事件驱动的）、以代码形式编写的合同（特殊的交易）。智能合约非常适合对信任、安全和持久性要求较高的应用场景，比如：数字货币、数字资产、投票、保险、金融应用、预测市场、产权所有权管理、物联网、点对点交易等等。
- 2. 智能合约的使用步骤



- 3. 合约编程语言：Solidity
- 智能合约的默认的编程语言是Solidity，文件扩展名以.sol结尾。Solidity是和JavaScript相似的语言，用它来开发合约并编译成太极链虚拟机字节代码。
- 4. 合约的编译
- 以太坊虚拟机上运行的是合约的字节码形式，需要我们在部署之前先对合约进行编译，可以选择Browser-Solidity Web IDE或solc编译器。

- 5. 合约的部署
- 总的来说，在以太极链上部署和运行智能合约需要以下几个步骤：
- （1）启动一个太极链节点（如occ）。
- （2）使用智能合约语言编写智能合约（如Solidity）。
- （3）使用solc编译器将编写好的合约代码转换成太极链虚拟机位码。
- （4）将编译好的合约代码部署到网上。
- （5）使用web3.js库所提供的JavaScript API接口来调用合约。
- 6. 合约运行
- 合约部署之后，当需要调用这个智能合约的方法时只需要向这个合约账户发送消息（交易）即可，通过消息触发后智能合约的代码就会在太极链虚拟机中执行了。

五 太极链关于“币”的论述

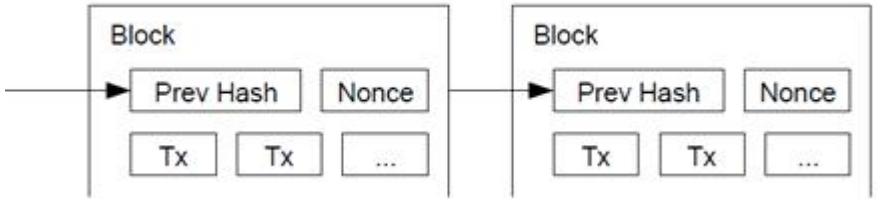
- （一）总述
- 古人说：无极而太极。太极动而生阳，动极而静；静而生阴，静极复动。一动一静，互为其根。分阴分阳，两仪立焉。阳变阴合而生水火木金土，五气顺布，四时行焉。五行一阴阳也，阴阳一太极也，太极本无极也。
- 五行之生也，各一其性。无极之真，二五之精，妙合而凝。乾道成男，坤道成女。二气交感，化生万物，万物生生而变化无穷焉。
- 唯人也得其秀而最灵。形既生矣，神发知矣，五性感动而善恶分，万事出矣。圣人定之以中正仁义而主静，立人极焉。
- 这段话，很重要，这个宇宙的根本来源和变化根源好像都讲到了，不过，本文并不是谈哲学，也不是谈宗教，落脚点却在最后一段话上：唯人也得其秀而最灵.....为什么这段话很重要呢？因为区块链起源于比特币，比特币是什么？它的重点在“币”这个字上，“币”就是钱，于是乎，区块链天生就和钱不可或分，如何做一个“义利结合，寓义于利，先义后利”的君子，并且有效地合理地使用钱，这是世界上最大最难的学问之一了，要靠“秀而灵”的我们的头脑了！不可利欲熏心，障碍了心智。
- 太极链具备以太坊的所有功能，同时又简化了一些功能，目前，以太坊用得最多的功能就是发TOKEN（类似于发自己或项目的数字货币），其实，这个TOKEN是一个极其简单的操作，在太极链中，这个动作已经格式化了，我们只需要输入简单的数字和名称就可以发TOKEN了，人人可以发TOKEN，而且性质和以太坊的TOKEN是一模一样的，这样就会有俩大好处：一个是人人会明白TOKEN的实质；另一个是非确有公信力之个人或者单位（项目）难以令人跟随；这样就会让有价值的变得量化或者更有价值，而没有价值的“空气币”就被从根本上杜绝了。

- （二）乾元通宝OCC
- 1. 释义
- 乾元通宝是太极链的内置本币，通常而言，太极链的本币应该姓“太极”才对，为何叫“乾元通宝”呢？我们首先要知道，太极链也是一条“文化之链”，要弘扬东方文化，所以，“乾元通宝”的命名，就具有东方文化的特性了！
- 世间万物，均来自于一个根源，这个根源古人说是“道”，今天可以勉强说是能上能下，能左能右，能变化万物的“能”，而这个“道”，这个“能”，在中国文化的《易经》系统里别有一名词，称为“太极”，太极是什么？按照《易经》的道理，万物统一在阴阳之中，而太极不属于于阴阳，“能阴能阳者，非阴阳之所能为”，这个能阴能阳者，就是“太极”。而乾，是阴阳八卦的第一卦，也是六十四卦的第一卦，乾是什么？《易经.系传》说：乾者，“万物资始”，“首出庶物，万国咸宁”，就是一切变化最初的来源，就我们宇宙而言，相当于整个的虚空，或者说是整个宇宙，不是没有，是什么都有，这就是“乾”的寓意。元者，元始也，元源也，也是一切之来源，一切之根源之意！一切之根源若何？一切之根源于道也，源于太极也，于人道而言，源于德也！“通”，就是“亨通”，“流通”，“通行”，有德方可通行天下，为天下之宝，所以说叫“乾元通宝”！
- “乾元通宝”的英文简称是“OCC”，英文全名是：Original Comm Cimelia.

- 2. 发行量说明
- “乾元通宝”一共发行6400万枚，因为太极生阴阳，阴阳生五行，五行生八卦，八卦而得六十四卦，在东方文化里，“数”是一个很奇妙的东西，万物皆有“定数”，6400万枚OCC，象征着64卦，可以“范围天地之化而不过，曲成万物而不遗”，可以为太极链“保驾护航”，通行天下，让所有的参与者获益。不惟是现实的数字资产的利益，也不惟是在太极链上布署高级智能合约带来的便利，更有很多其他非同寻常的利益，只要我们多多研究太极链的精神和数理，一定会利益无穷。
- 3. 用途
- 乾元通宝之用途：太极链网络包含自身的内置货币“乾元通宝”，乾元通宝扮演双重角色，为各种数字资产交易提供主要的流动性，更重要的是提供了支付交易费用的一种机制。可以确保太极链的运行畅通无阻。

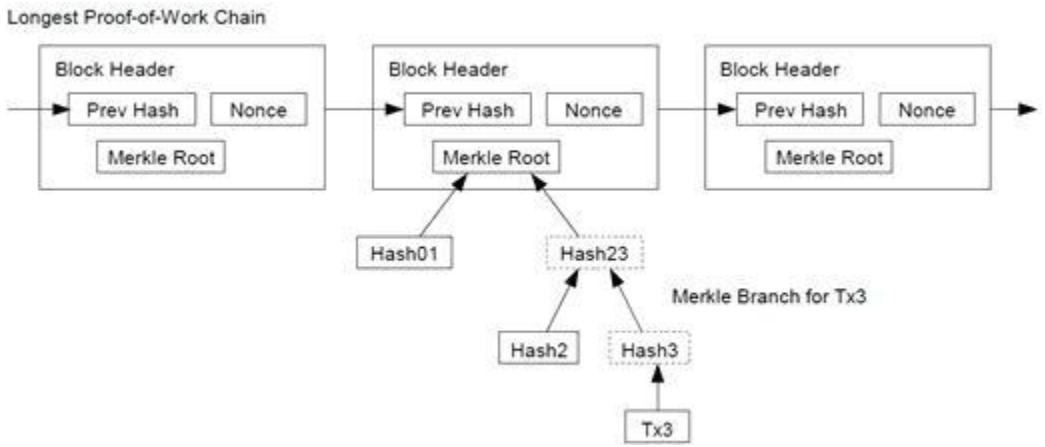
六 关于挖矿

- （一）挖矿
- 比特币是采用的工作量证明(Proof-of-Work即POW)挖矿
- 计算一个随机数(Nonce)，将随机数与区块头一起计算随机散列值（Hash），该散列值要满足以N个0开头（N为变量，可通过N来控制计算难度，N越大，难度越大），此即为“挖矿”的内部原理。

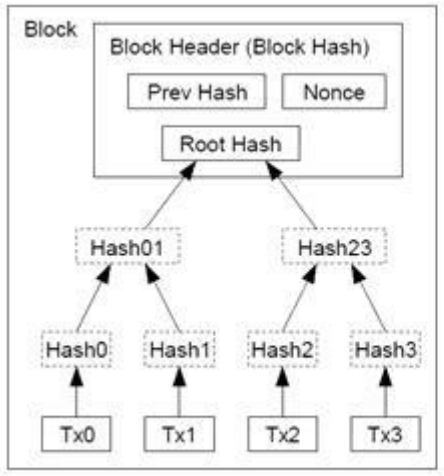


- （二）POW意义非凡
- 1. 保证区块链（Blockchain）的不可篡改性，由于区块形成了链条，如果要修改区块，必须重新完成之前所有的工作量，所以随着区块链高度越高，越旧的区块越难以篡改。
- 2. 工作量证明的本质是一CPU一票（与传统的一IP一票不同，攻击者要获得更多的票数需要投入大量的成本），如果大多数的CPU为诚实节点，那么正确的链条将以最快的速度延长。
- 3. 比特币区块链的“时间戳服务器模型”能保证账本的顺序和真实性，但是无法阻止人为的创造多个账本，而这些账本中只能有一个是被大家认可的，所以必须创造一种共识机制。比特币的共识机制即为工作量证明（POW），即工作量（Hash计算）最大的那个账本是大家公认的正确账本。
- 4. 工作量证明有一个风险，就是有人如果控制了全网大量的算力（如超过51%），实际上他可以控制大部分的记账权，对于比特币网络将产生风险。但是比特币的设计将这种风险产生的后果降到了较低的水平：
- （1）由于仅有算力，没有私钥，无法随意掠夺别人的货币。
- （2）虽然他可以拒绝别人的交易计入账本，但这种破坏实际并不会对别人造成货币的损失。
- （3）他还可以试图进行双重支付，但如果在大额交易中对方进行多个块（如6个以上）确认来验证交易，仍然很难完成双重支付。并且这种攻击发生会很容易被察觉，比特币社区可以快速做出应对。

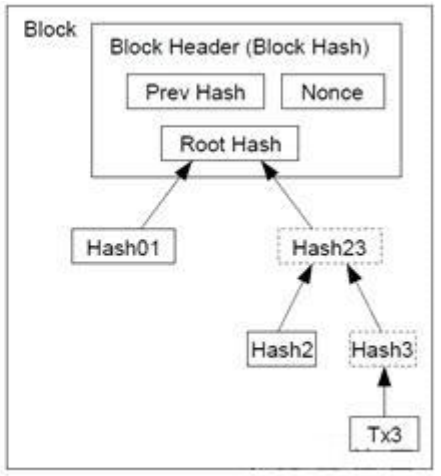
- 回收硬盘空间：交易信息构成Merkle树的形态，通过merkle树的原理可知，只需要根节点(root)与路径即可验证交易的正确性，使得用户只需要存储区块头（含有Merkle root），在需要时获取Merkle树路径即可校验一笔交易。



- 不含全部交易信息的区块头(Block header)仅80字节，区块生成速率约为10分钟一个，每一年只产生数据4.2MB；
- 简单的支付确认：在不运行完整网络节点的情况下，也能够对支付进行校验。节点只需保留区块头，通过merkle的分支校验某次交易是否存在即可。

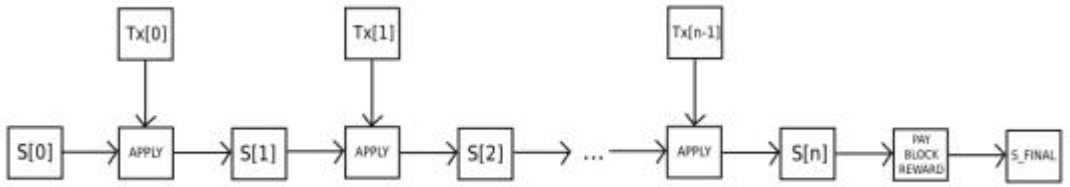


Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

- （四）太极的区块链和挖矿
- 与以太坊非常相似，太极链的区块链在很多方面类似于比特币区块链。它们的区块链架构的不同在于，太极链的区块不仅包含交易记录和最近的状态，还包含区块序号和难度值。太极链中的区块确认算法如下：
- （1）检查区块引用的上一个区块是否存在和有效。
- （2）检查区块的时间戳是否比引用的上一个区块大，而且小于15分钟。
- （3）检查区块序号、难度值、 交易根，叔根和瓦斯限额（许多OCC特有的底层概念）是否有效。
- （4）检查区块的工作量证明是否有效。



- （5）将S[0]赋值为上一个区块的STATE_ROOT。
- （6）将TX赋值为区块的交易列表，一共有n笔交易。对于属于0……n-1的i，进行状态转换S[i+1] = APPLY(S[i],TX[i])。如果任何一个转换发生错误，或者程序执行到此处所花费的瓦斯（gas）超过了GASLIMIT，返回错误。
- （7）用S[n]给S_FINAL赋值, 向矿工支付区块奖励。
- （8）检查S-FINAL是否与STATE_ROOT相同。如果相同，区块是有效的。否则，区块是无效的。
- 这一确认方法乍看起来似乎效率很低，因为它需要存储每个区块的所有状态，但是事实上太极链的确认效率可以与比特币相提并论。原因是状态存储在树结构中（tree structure），每增加一个区块只需要改变树结构的一小部分。
- 因此，一般而言，两个相邻的区块的树结构的大部分应该是相同的，因此存储一次数据，可以利用指针（即子树哈希）引用两次。一种被称为“基数树”（“Patricia Tree”）的树结构可以实现这一点，其中包括了对梅克尔树概念的修改，不仅允许改变节点，而且还可以插入和删除节点。
- 另外，因为所有的状态信息是最后一个区块的一部分，所以没有必要存储全部的区块历史-这一方法如果能够可以应用到比特币系统中，经计算可以对存储空间有10-20倍的节省。

七 未来展望

- 太极链无论现在还是将来，都会是一条一直在发展中的链，未来的构想，远不止紫皮书相关章节讲到的1.0到3.0的范围,我们将持续更新,而更大的理想是:太极链正在酝酿“互链网”这个概念,欲成为“区块链万链之枢纽”。这也是“太极链”取名的来由之一，也是其题中就有之义了。
- “互链网”简单来说就是“链间互链”，所有的区块链都需要遵守一个区块链的协议，类似于邮件系统的“SMTP协议”，或者互联网的“IP协议”，它必须高于链这个层次，要把下层的链当操作系统 API 来调度。这个协议可以叫“互链通协议”。
- “互链”的意思是代表区块链所需要的基础设施，与今天的互联网不同，是针对“互链网”的需求而匹配的。互联网，主要是信息互联网。信息互联非常重要，但是区块链是价值互联，价值互联需要更强的基础设施。区块链承载价值和共识，区块链价值的流转的是信任。信息与价值的传递，最大的差别是“互联”与“互链”的差别。写资料可以随便，但是区块链是帐本，不能随意，环环相扣是为链，信任和价值要链接在一起，环环相扣。
- 目前，链间价值的互通，比较勉强的，是跨链技术。
- 那就让我们先来谈谈跨链技术吧：
- 跨链技术，早期有 Blockstream 提出侧链技术，以及比特币和以太坊两大公链之间充当传令兵的 BTC-relay，到现在有 RootStock、Polkadot，这些都是着眼于跨链通讯的。

- 目前出现的几种跨链技术，都是在解决方案的层面，而不是协议层面。解决方案，就是我有一个问题，我想个可行的办法去解决这个问题。协议是要为着一个目标，在多利益关联方之间，制定一套游戏规则，只要遵守这套游戏规则，大家就可以互通共赢。
- 比如侧链技术，其实本质上就是主侧链之间双向锚定，相互信任。主链要向侧链转移资产时，通知侧链自己已经将一部分主链资产锁定，而侧链可以去检查主链资产的锁定状态，然后在自己的链上发行等值的侧链资产。这个过程宏观来看就是完成了资产的跨链转移。所以这只是一套区块链层面的技术，需要主侧链彼此了解，相互配合。而不是协议。
- 作为链间通讯解决方案，它规模性不行。两条链的时候很简单，一主一侧就可以了，如果是几十条链几百条链，怎么办？那只有围着一条中心主链来转。那这相当于什么呢？相当于每一个中心主链跟其侧链之间又打造了一个大一点的小宇宙，但是跟外界还是隔绝的。
- 同时，它不能够对上层应用提供强有力的抽象。你在这套体系里做出来的智能合约和 Dapp，还是局限在具体链上的。你的智能合约能运行在不同的链上，甚至同时运行在多条链上吗？恐怕是不行的。

- 这跟互链网的愿景，想去甚远
- 所以目前的跨链技术不能成为“互链网 IP”的 细腰。因为这是跨链技术而非协议。
- 问题在于：链间互链的问题，根本就不应该是在链这个层面解决，它必须高于链这个层次，要把下层的链当操作系统 API 来调度。
- 同时，在横向上，太极链将研究如何与各类产业结合，开发无穷的区块链应用，也将结合社会管理现状，结合区块链的内在规则做相应的应用。
- 这些是太极链持续的研究方向了。所以，太极链，永远都在生生不息之中。
- 让我们期待更大的惊喜吧！

八 创始人

- 鬼谷子，紫阳真人，玄玄道长

九 参考资料

- 1. 《易经系传》　　作者：伏羲 孔子
- 2. 《原本大学微言》　　作者：南怀瑾
- 3. 《比特币白皮书》　　作者：中本聪
- 4. 《以太坊白皮书》　　作者：Ｖ神
- 5. 《图灵的秘密:他的生平、思想及论文解读》
- 2012-11 Charles Petzold、 杨卫东
- 6. 《密码工程:原理与应用》
- 2018-01尼尔斯·弗格森 (Niels Ferguson)、 布鲁斯·施奈尔
- 7. 《算法导论》(原书第3版)
- 2013-07　Thomas H.Cormen、 Charles E.Leiserson