Bytom 比原链
一个多元比特资产交互协议

摘要

Bytom Blockchain Protocol（简称比原链：Bytom）是一种多元比特资产的交互协议，运行在比原链区块链上的不同形态的、异构的比特资产（原生的数字货币、数字资产）和原子资产（有传统物理世界对应物的权证、权益、股息、债券、情报资讯、预测信息等）可以通过该协议进行登记、交换、对赌、和基于合约的更具复杂性的交互操作。连通原子世界与比特世界，促进资产在两个世界间的交互和流转。比原链采用三层架构：应用层、合约层、数据层，应用层对移动终端等多终端友好，方便开发者便捷的开发出资产管理应用；合约层采用创世合约和控制合约进行资产的发行和管理，在底层支持扩展的 UTXO 模型 BUTXO，对虚拟机做了优化，采用自省机制以防止图灵完备中的死锁状态；数据层使用分布式账本技术，实现资产的发行、花费、交换等操作，共识机制采用对人工智能 ASIC 芯片友好型 POW 算法，在哈希过程中引入矩阵和卷积计算，使得矿机在闲置或被淘汰后，可用于 AI 硬件加速服务，从而产生额外的社会效益。

1 比原链的使命、目标与创新

1.1 问题总览

总的来说，信息革命极大的改变了我们生活的世界，纯粹原子性构造世界的主宰地位正受到挑战，在大数据奇点临近和大规模计算能力提升的时代背景下，互联网正面临从“信息即权力”到“计算即权力”的过渡阶段，而世界经济结构与权力迁移更多的由比特信息构成。包含“负熵”信息流、比特流成为个人及企业、机构赖以生存运作的一部分。演进的路线逐步从早期的：

“比特工具”时代：比特作为一种辅助性提高效率的产物，例如：excel 表格、email 邮箱；发展到后续的 **“比特货币”时代**：比特形式存在、没有物理载体及介质对应的价值符号例如：比特币、以太币以及各种公有链、联盟链代币；再到更加广泛多元的 **“比特资产”时代**：一切有价值，可交换的原子资产，例如现实经济的收益

权、股权、债权、证券化资产等， 都可跃迁到不可篡改、可追溯、信息对称的区块链分布式账本上，通过可编程智能合约与金融、博彩、保险等预测市场产生交互。

然而，从原子世界出发购买一个软件（比特工具）、数字货币（比特货币）都已经有成熟的软件商店例如 Appstore，交易所例如 Coinbase，但对于多元化的比特资产的交易、交互却并没有一套完整的、行之有效的协议系统承载其交互。与以太坊等通用型智能合约平台不同的是，比原链被设计为针对资产领域的专用型公链平台，并试图解决以下问题：

- 如何通过区块链技术，让比特资产实现原子资产的不可复制性？
- 如何建立原子资产与比特资产的映射关系，并解决合规性问题？
- 如何打破原子世界与比特世界的鸿沟，促进资产在链上链下的高效流通？

1.2 使命陈述

“我们的任务是连通比特世界与原子世界，建造起一个多元化资产的登记、流通的去中心化网络”。

Bytom 将极大的推动现有的价值属性的比特信息、比特资产的交换、交互及流动。通过合约和配置，也将产生新的比特资产。Bytom 还将以去中心化的形式、基于市场的管理协议去创造应用，并同时为本地和全球的比特经济参与者提供独特的激励。Bytom 作为一种媒介，已经充分准备好成为一个促成信息获利的经济体，一个信息资产效能的放大器。在未来，这些信息资产不仅会为现有的日常工作生活所用，也可以成为人工智能、物联网设备的“数据食物”的提供者，以进一步加速其对原子世界的影响力。

1.3 核心目标

1.3.1 建造多元化比特资产登记的标准

Bytom 旨在建立一个全球性开放的 Byte Assets 登记平台。并让创建和定义、生成一种比特资产更加便捷，也更容易为用户所理解。

1.3.2 建造多元化比特资产的交互工具

从最基本的资产的交换工具（不同形态的数字资产间按协定进行交换、所属权的变更）、Bytom 还将支持较为复杂的交互形式，例如 ：

A 触发工具：资产依照合约规定的投票，产生确定性 Y / N 布尔结果或数值结果，以激活原子世界的参与方共享数据集；

B 预测工具：例如通过零和博弈，双方或多方对赌，产生某场航班是否延迟、两位候选谁将胜出的预测信息，将此预测信息用于现实世界的金融对冲、保险等领域。

1.4 主要创新

（1）与比特币 UTXO 的设计兼容

比原链由三层组成：数据交易及传输层、合约层、资产交互层。资产交互层通过调用合约来对资产进行操作，其中在在数据交易及传输层，兼容比特币的 UTXO 模型和交易数据结构，以实现高速并发和可控匿名。

（2）通用地址格式

比原链钱包的设计中将引入 BIP32，BIP43，***BIP44***[1]理念，用 Hierarchical Deterministic Wallets （or “HD Wallets”）提供对多币种、多账户、多地址、多密钥的支持。BIP44 提供了一种 5 层路径建议：（1）确定路径规则；（2）币种；（3）账户；（4）找零；（5）地址索引。用户只需要保存一个主私钥，就能控制所有币种、所有账户的资产钱包。BIP44 对找零机制提供了很好的支持，用户只要不用同一地址多次收款，就可以避免同一私钥多次签名，从而规避私钥暴露的风险。

（3）支持国密标准

比原链的资产控制和操作中涉及到私钥、公钥、地址体系。传统的比特币代码实现中基于椭圆曲线函数加密 ECDSA 和 SHA256 散列。在比原链中将进一步支持 ***国密 SM2 椭圆曲线公钥密码算法***[2] 和 ***SM3 密码杂凑算法***[3] 。在实现同样的计算复杂度时，SM2 在私钥的处理速度上远快于 RSA、DSA 算法，加密效率更高。SM3 算法的压缩函数与 SHA-256 的压缩函数具有相似的结构，但是 SM3 算法的设计更加复杂，比如压缩函数的每一轮都使用 2 个消息字。

（4）资产命名采用 ODIN 标识

链上资产的命名采用 ODIN（Open Data Index Name）开放数据索引命名标准，利用区块链透明可信、不可篡改特性，保障资产的全网、全链唯一性。与其它基于区块链的标识解决方案不同的是，ODIN 基于比特币区块链，支持扩展多级标识引入其它区块链（公有链、联盟链、私有链），不是以抢注字符串的方式，而是用区块记录位置作为标识名称。

（5）人工智能 ASIC 芯片友好型 POW 算法

采用对人工智能 ASIC 芯片友好型 POW 算法，使得矿机在闲置或被淘汰后，可用于 AI 加速服务。

比特币矿机和人工智能深度学习具有可比性，它们都是依赖于底层的芯片进行大规模并行计算。深度学习算法绝大多数可以被映射为底层的线性代数运算。线性代数运算有两大特点：一是 Tensor 的流动非常规整且可预期；二是计算密度很高。这两大特点使得 AI 深度学习特别适合做硬件***加速***[4]。

比特币矿机芯片历经了 CPU、GPU、FPGA 和 ASIC 四个阶段（图 1）。在 CPU、GPU 时代，挖矿门槛较低，家用台式机或带有独立显卡的笔记本都可以用来挖矿。随着 FPGA、ASIC 矿机的面世，比特币矿业的摩尔定律高速增长，目前矿机算力都达到了 GH/S 的级别，硅片加工精度已经从 130nm 提升至 14nm，接近目前半导体技术的极限。但是，工作量证明机制被人诟病的是，矿机哈希计算的应用范围太窄，基本只能用于挖矿，造成极大的硬件与能源浪费。

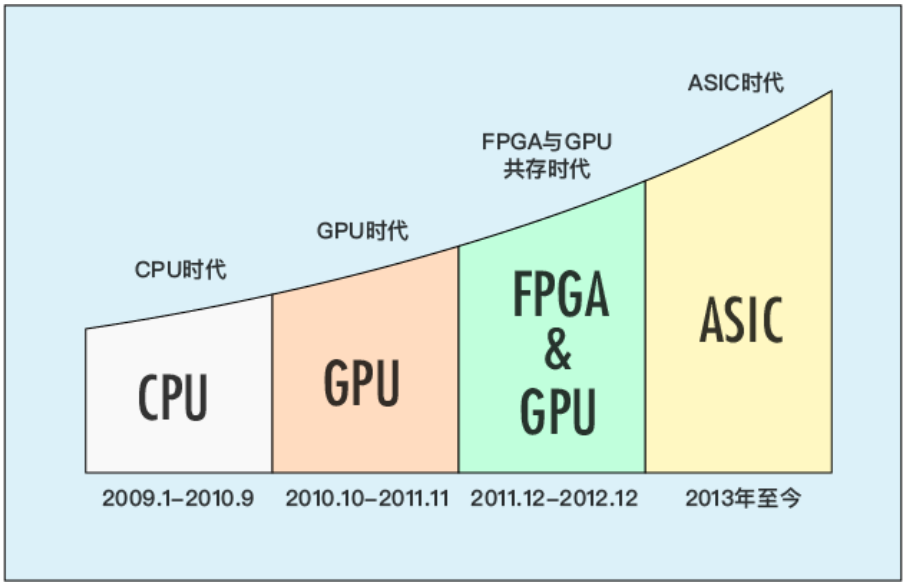

图 1

如果我们在挖矿的哈希过程中引入矩阵运算与卷积运算，使得矿机对人工智能 ASIC 相对于 GPU、CPU 更友好，那么，区块链共识所需要的计算量同样可以应用于 AI 硬件加速服务，从而产生较大的社会效益：一方面，矿机市场会刺激人工智能市场，扩大对深度学习 ASIC 芯片的需求，正如目前显卡友好型 PoW 区块链，对显卡市场的促进作用；另一方面，被淘汰或闲置的矿机可应用于 AI 硬件加速服务，节省挖矿成本，形成双赢局面。

（6）使用侧链支持跨链资产交易及分红

为对其他链上资产进行操作，在比原链上开发者可以创建一种小型版本的 X 链（其他链）中继器 XRelay，比原链上的 Dapp 开发者可以从智能合约向 X 链中继器进行 API 调用，来验证 X 链网络活动，实现跨链通信。继而在合约中完成交易和分红操作。

（7）类“隔离见证”设计

比原链设计了一种多种资产可以交互的分布式账本协议。用该协议的多条链可以独立的存在，并且可以跨链交易， 这样不同的运营商可以相同的形式交互。坚持最小权限原则，其中比原链的区块设计中将数据和见证（Witness）、签名部分分离，以实现资产的管理和分布式账本同步控制相分离。实现了更好的可编程性和合约支持，并且为之后的旁路通道预留接口。

链协议允许任何网络参与者通过编写自定义 “发布程序” 来定义和发行资产。一旦发行，资产单元由 “控制程序” 控制。控制程序是用图灵完备的编程语言实现，该语言可用于编写复杂的智能合约。

（8）增强的交易灵活性

BUTXO 与以太坊账户模型不同，可以并行验证交易，只要用类似于 nonce 的机制保证每一个未花费 outputs 最多只能被一笔交易所引用。此外，比原链支持超级轻客户端，天然的比以太坊瘦，建立轻量级的世界状态，参与者只需要记住未花费的 outputs 即可，因为交易会自带其他相关信息（如资产 ID，份额，控制程序）。比原链的另外一个特点是：compact 验证，只允许客户端验证块中所相关的交易，而不需要验证所有的交易，只要信任签名者的数量即可。整个过程是用 Merkle 证明，客户端也可以将监视整个区块链的任务委托给自己信任的服务器，区块可以通过软分叉的方式向前向后版本兼容。比原链不仅支持在实现本协议的区块链间通信（但需要保证全局资产 ID 的唯一性：每一条分链是从另外一条链的块高度分叉出去的，根据这点能保证资产 ID 唯一），也支持不同的协议的链互相交互，因为 BVM 提供了足够多的指令。

2 平台模型：三层结构

比原链将采用三层结构（图 2）：

i. 应用层：支持开发可编程的分布式应用，调用合约进行资产的登记、销毁和交易、分红
ii. 合约层：账户体系、合约代码支持
iii. 账本层（数据层）：无需许可的公有链层，POW 共识

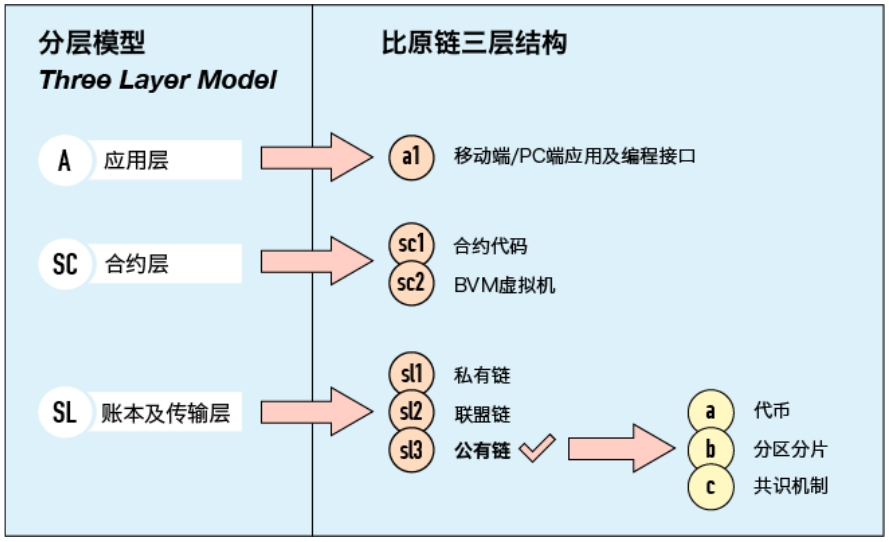

图 2

2.1 应用层面：

比原链提供多种形式的 PC、WEB、移动端应用以方便调用合约进行资产操作。我们通过对区块链底层技术的封装，降低应用层面的使用门槛，为开发者、资产发行方提供更灵活、更友好的接口，使得开发者、资产发行方可以专注于商业模式与业务逻辑上的创新。

2.2 合约层面：合约层面设计

2.2.1 创世合约

创世合约是比原链上一个特殊类型的合约种类，是可以发行并审核智能合约的合约，将由开发者将保留部分权限，例如私钥、作用域等，并有一定的规范和自动化审计功能，以确保链上资产符合相应的规范和模版被登记和发布出来。创世合约的底层实现，会调用到数据传输层中的发布程序：Asset Issuance Program。

2.2.2 普通合约

普通合约的功能有两种，进行资产的交易和分红的设置、认定，此类权限放开，每个合约相当于现实中的一个基金。如果合约中需要开发或引入一种新的资产，需要向创世合约提交请求，经审核通过后方能发布到链上。普通合约的底层实现会调用到数据传输层中的控制程序：Asset Management Program。

2.3 账本层（数据层）

在账本及数据传输层面，比原链采用公有链上较为成熟的 POW 机制，并加以改进，采用对人工智能 ASIC 芯片友好的算法。并采用分区分片机制，加速交易处理的效率，同时保证数据的一致性。

3 比原链的主控程序与数据结构

这一部分主要运作在***数据账本层面***[5]

比原链的主控程序包含三个部分，分别是

- Asset Issuance Program 负责资产的发行
- Asset Management Program 负责资产的花费、交换等操作
- Consensus Program 负责判别哪些新的区块可以被纳入比原链中，目前采用 POW 机制

3.1 多元化比特资产的发行

比原链将支持多种类型的数字资产。每种资产都将由一个资产 ID 进行标识，其中资产 ID 将是由一个 256 位 的字符串，区分不同的资产类型。根据不同资产 Asset_ID，我们可以确立该类资产 所属类型，并关联到该类资产的：资产生成程序（Asset_Issuance_Program 专门负责生成新的资产单元）、资产操作程序（Asset_Management_Program 对接受到一组资产进行控制和操作）。

比原链上运行有两类资产：比原币（Bytom Token，简称 BTM）与资产（Assets）。

3.1.1 代币 Token

比原链上的代币即比原币，是比原链上对于打包交易者以及系统参与节点分发的一种特殊类型的 Token，采用 POW 机制，鼓励随机匿名的矿工参与到整个生态中，按照预定发行曲线分发而生成。

比原币的主要用途有：

i. 资产交易的手续费；
ii. 收益权资产的分红；
iii. 资产发行的押金；

以收益类资产的分红为例，若资产发行方决定以比特币作为分红，可通过侧链锁定相应额度比特币，按市场汇率转化为比原币，再发放至资产所有者的地址上。此过程由合约调用 XRelay 进行跨链操作完成，例如与 BTC、ETH 兑换分别通过 ***BTCRelay***[6]、ETHRelay 完成（图 3）。

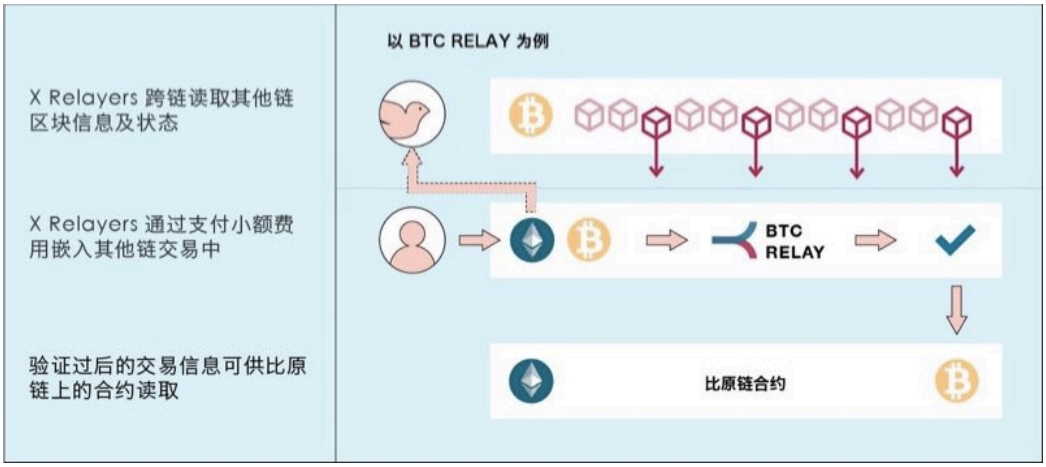

图 3

3.1.2 资产 Assets

比原链上的资产有三种类型：

i. 收益类资产：收益类资产包括电影、民宿等众筹形式的收益权资产、地方政府固定投资的长期收益权、不良资产收益权等。

ii. 股权类资产：股权类资产包括非上市公司的股权、私募基金投资的股权、互联网非公开投资的股权等，股权类资产的转让需要完成投资人资格认定。

iii. 证券化资产：证券化资产包括应收账款、汽车贷款等未来能产生可预见现金流，通过结构化设计进行信用增级，在此基础上所发行的资产支持证券。

3.2 链上资产的交换

本节中我们将讨论比原链的最基本的功能，即 1.3.2 中描述的 “资产交换” 部分，这将在比原链的第一个版本中得以实现。

资产收益权、持有权、使用权等的交易：采用合约内部账户转账的登记形式。

资产的赎回：采用合约转出比原币的形式。

账户是比原链内部抽象出的概念，属于合约层概念，每个账户在数据账本层面将对应到一组 BUTXO，该账户下所有 BUTXO 资产数目总和形成该账户的余额。

以下为比原链数据模型的基本概念：

交易 Transactions

交易是比原链资产的一个基本的操作事务，它是一个含有输入值和输出值的数据结构。

输入 Inputs

可以是一笔或多笔不同类型的数字资产，或是某笔交易的输出；

输出 Outputs

确定了交易后资产结果，是一个资产操作程序，规定此项输出的未来花费的方式。

下图（图 4）展示的是比原链上扩展的 BUTXO，它对比特币公链上传统的 UTXO 结构进行了扩展，可以兼容多种类型的比特和原子资产。

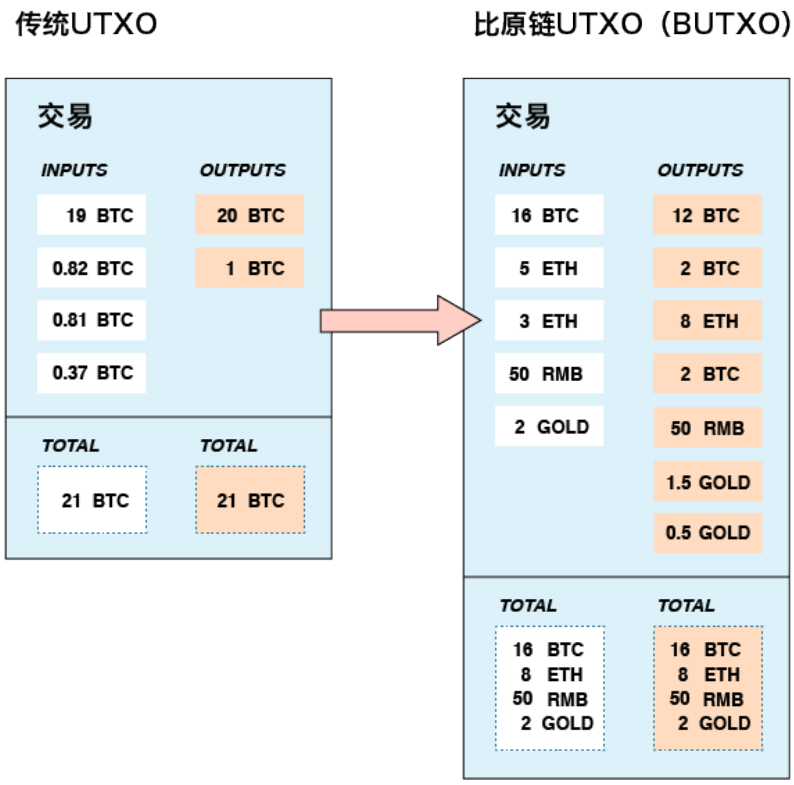

图 4

每个交易中的输入部分必须是一组新生成的资产单元，或是之上一组 BUTXO 经过一经过资产操作程序运算返回的结果，这两种输入必须经由上面提到发行程序验证通过。发行程序的验证过程是可以向交易中的 验证域（Witness Field）部分传递参数，然后验证部分通过，则进行交易（图 5）。这一部分有些类似于比特币公链 BIP141 提出的隔离验证思想。

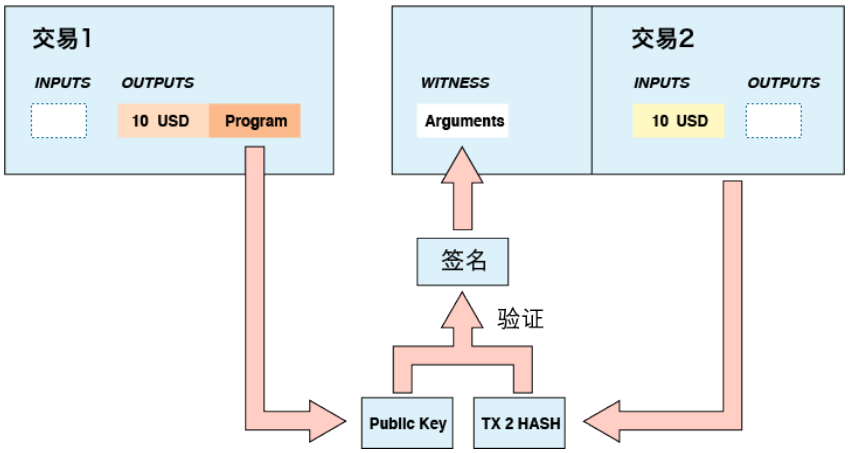

图 5

例如资产生成程序和资产操作程序可以发起一个真实性验证，给定一条消息，将消息生成 Hash 值，然后对此 Hash 值进行签名。由签名（signature）与 Hash 值，便可验证此签名是否由公钥对应的私钥签名。

BUTXO

为了防止双花，并增加交易的并发性和处理效率。比原链中引入了扩展的、支持多种资产类型的、一个交易的未花费交易输出 BUTXO （Bytom Unspent Transaction Output），它是比原链中一个交易的基本单位（图 6）。一旦一个交易使用了某一个特定的输出，则其他交易不能使用相同的输出。整个比原链都维护着一个全局的 BUTXO 池，所有的区块的输入其实都会关联到现有的一个或多个 BUTXO，一旦一个交易得到了确认，则这个交易中被使用的输出则被销毁池中移除，新的未经花费的 BUTXO 输出则被加入。

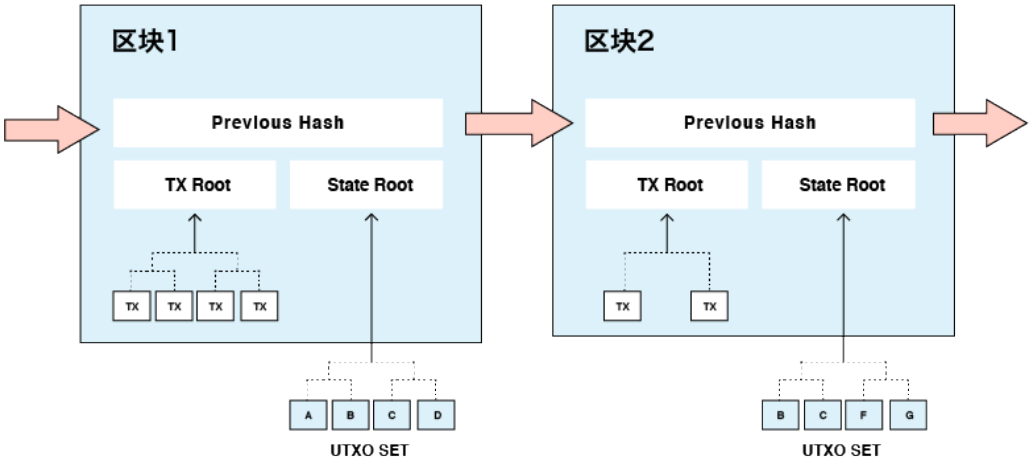

图 6

区块

比原链中的一个或多个交易被打包到区块这样的数据结构中。其中，每个区块的区块头中有上一个区块的哈希，依次链接，以确保整个区块组成的区块链不可篡改。每个区块中则包含有该区块的所有的交易的哈希，以及现有状态 BUTXO 的哈希快照。这两个哈希分别对应两个默克尔树（Merkle Tree）的树根。通过这个两个默克尔树可以对交易和 BUTXO 进行简化的判别和验证。

3.3 共识机制

为保证整个区块链的交易数据安全性，区块的生成需要遵守一定的共识程序（Consensus Program ）。一个安全的资产区块链共识程序应包括以下属性：

（1）验证交易真实性：交易真实性验证只与公钥—私钥对有关，单个参与者可以生成和使用多个密钥对。

（2）不可否认性：事实发生后，参与方不能否认交易发生过；

（3）完整性：事实发生后，交易不能被篡改，交易一旦被创建，就被广播到点对点网络中。

按照***最小可行区块链原理***[7]，交易需被打包成区块，使得交易费用相对于资产本身的价值是低廉的；有效区块需有效的工作量证明，使得工作量产生很难，但验证起来很容易；工作量通过哈希现金算法实现，建立在能源成本之上，从而提高生成有效区块的成本，使得恶意攻击者难以承受攻击的成本。

由于比原链专注于做资产的区块链解决方案，需要在多节点上达成较强的共识，整个系统不容易受到女巫攻击（Sybil Attack）和 51%攻击，所以对***不可能三角***[8]中的安全（全局一致性）、去中心化要求较高，一定程度上牺牲了高效。比原链在比特币公链、以太坊公链所采用的 POW 机制基础上，实现对人工智能 ASIC 芯片友好的共识算法，使得挖矿算力可以被应用于 AI 硬件加速领域，从而解决 PoW 机制的硬件消耗问题。

3.4 虚拟机（BVM）

Bytom 的虚拟机是一个栈式状态机：任何指令都在该栈中执行。BVM 的指令集是图灵完备的，为了防止死循环，采用了 run limit 来限制陷入死循环，协议允许网络去达成共识设置该 run limit，根据运行消耗来定价每一条一条指令的 run limit。这非常类似于以太坊的 gas 机制，和以太坊不同的是 BVM 不会在每笔交易中给 run limit 计

费。BVM 指令集包含了 push， pop 等基本指令集，同时还包括了 SHA3，CHECKSIG，CHECKMULTISIG 等复杂的数学加密运算。

自省功能

交易自省：可以在执行过程判断是否超过预定的时间，也可以增加自带控制程序，来对（价格，资产，运行过程， 索引）做一定自由控制。

区块自省： 自省指令集（BLOCKHASH，NEXTPROGRAM），只能在共识程序中执行。

因为丰富的指令集，可以组合使用完成不仅仅是交易签名和验签的功能。如：多重签名，提前部署（比如类似微信红包功能，A 给 B 发送交易，需要 B 确认才能上链）CHECKPREDICATE 提供了强大的其它跨链功能，包括实现类似于 BTCRelay 的功能。

4 应用场景

4.1 场景一 收益权资产管理

比原链可以用于收益类众筹项目的管理。区块链公开透明的特性，消除了众筹发起、投资以及后续资金使用过程中的信息不对称，降低了人们的信任成本。基于比原链提供的可编程接口，可以在众筹资产发行时内置智能合约，真正做到资金的专款专用，让投资人没有后顾之忧。智能合约还可以保证：如果你没有达成预定的目标，资金可以自动退回到支持者的账户。这些都不需要第三方背书和担保，不需要给第三方支付佣金。

通过比原链管理收益类众筹项目的优势有：（1）透明的规则和审计：当投资者使用基于比原链链技术支持的众筹项目，会留下了永久不变的公开记录，这个记录不能被篡改，也不会丢失。这些资金的事后使用情况也同样保存在一个任何人都可以获取的公开透明的账本中。这些特性提供了传统支付手段和事后审计所不能达到的信任水平与安全水平。（2）更好的流通性：众筹的支持者可以快速、简单地将众筹到的收益权在比原链上与其他人进行交易，交易可以通过去中心的点对点形式完成，业务通过比原链的担保交易完成。

4.2 场景二 非上市公司股权管理

非上市企业由于资金、利润方面的限制，在股权、期权、资金、流程方面的管理往往比较混乱，股东名册缺乏透明度与公信力，股权流动性差，股东难以通过投票行

使监督权。比原链为非上市企业提供股权登记和流转平台，所有股东信息在区块链上公示，从根本上达到确权的目的。企业可通过比原链降低股权、期权管理成本，期权成熟计划管理、协议的在线生成、授予、审批和签署都可以通过智能合约自动执行；律师在向企业提供法律服务后，可直接在比原链上完成签章授予等操作；股东可通过私钥的签名来远程完成股东大会的投票；公司治理结构的变动可通过线上智能合约+电子签的方式完成，从而免去了繁杂的文书工作。

比原链还适用于私募基金管理。私募基金管理人使用比原链发行私募基金，在智能合约中制定基金的资产审计、投资人回馈规则、回购规则、交易规则等，将使得整个管理严格执行，公开透明。基金份额变得更易转让和交易，投资人可以放心的购买长期股权投资基金，而无需担心不时之需，通过比原链的交易转让系统，可以随时将基金溢价或折价转让。

4.3 场景三 证券化资产管理

资产证券化（Asset Backed Securitization 简称 ABS）是指将缺乏流动性，但具有未来现金收入的资产打包起来，建立资金池并通过结构性重组方式，将其转变成可以在金融市场上出售和流通的证券。

证券化有三个步骤：第一步是发起人把这个资产扩展隔离到特殊目的载体，第二步是把这个特殊目的载体的资产分拆份额，第三步是交易。传统方式中，这个流程手续繁杂且效率低下。一般公司的证券发行，必须先找到一家券商，公司与证券发行中介机构签订委托募集合同，完成繁琐的申请流程后，才能寻求投资者认购。而且证券一旦上市后，交易更是极为低效，证券交易日和交割日之间存在数天的时间间隔。而区块链产生后，ABS 可以简化为三个步骤：一是确权对应；二是代币化，把资产分割成货币或 token；三是智能合约的交易。

通过比原链管理证券化资产，可极大的提高 ABS 资产运作的效率、安全性和可追溯性，实现交易数据的安全存储，保证信息不可伪造和篡改，并自动执行智能合约。ABS 交易过程中所有市场参与者，通过分布式账本和共识机制保持资产登记与交易信息的同步，有效解决了机构间费时费力的对账清算问题。

参考文献：

[1] ***BIP44*** https：//github.com/bitcoin/bips/blob/master/bip-0044.mediawiki

[2] ***SM2 椭圆曲线公钥密码算法*** http：//www.oscca.gov.cn/News/201012/News_1197.htm

[3] ***SM3 密码杂凑算法*** http：//www.oscca.gov.cn/News/201012/News_1199.htm

[4]***王逵 《CPU 和 GPU 双低效,摩尔定律之后一万倍》*** http://dwz.cn/67GUGv

[5] ***Chain*** https：//chain.com/

[6] ***BTCRelay*** http：//btcrelay.org/

[7] ***Ilya Grigorik《最小可行区块链原理》*** https：//www.igvita.com/2014/05/05/minimum-viable-block-chain/

[8] ***长铗《不可能三角：安全，环保，去中心化》*** http：//www.8btc.com/impossible-triangle