# Back to Basics 中美区块链产业的发展演变及产品设计启示

on Bytom's Whitepaper

巴比特执行总裁 段新星

# China Is Developing its Own Digital Currency

Bloomberg News
2017 M02 24 00:05 GMT+8

- PBOC cryptocurrency could give unprecedented read on consumers
- Payment platforms like Alipay, WeChat set to face competition

Bitcoin:Method,of,Payment

# New Japan law recognizes bitcoin as method of payment

BY **Jasmine Solana** ON **March 31, 2017**

TAGS: **BITCOIN**, **JAPAN**

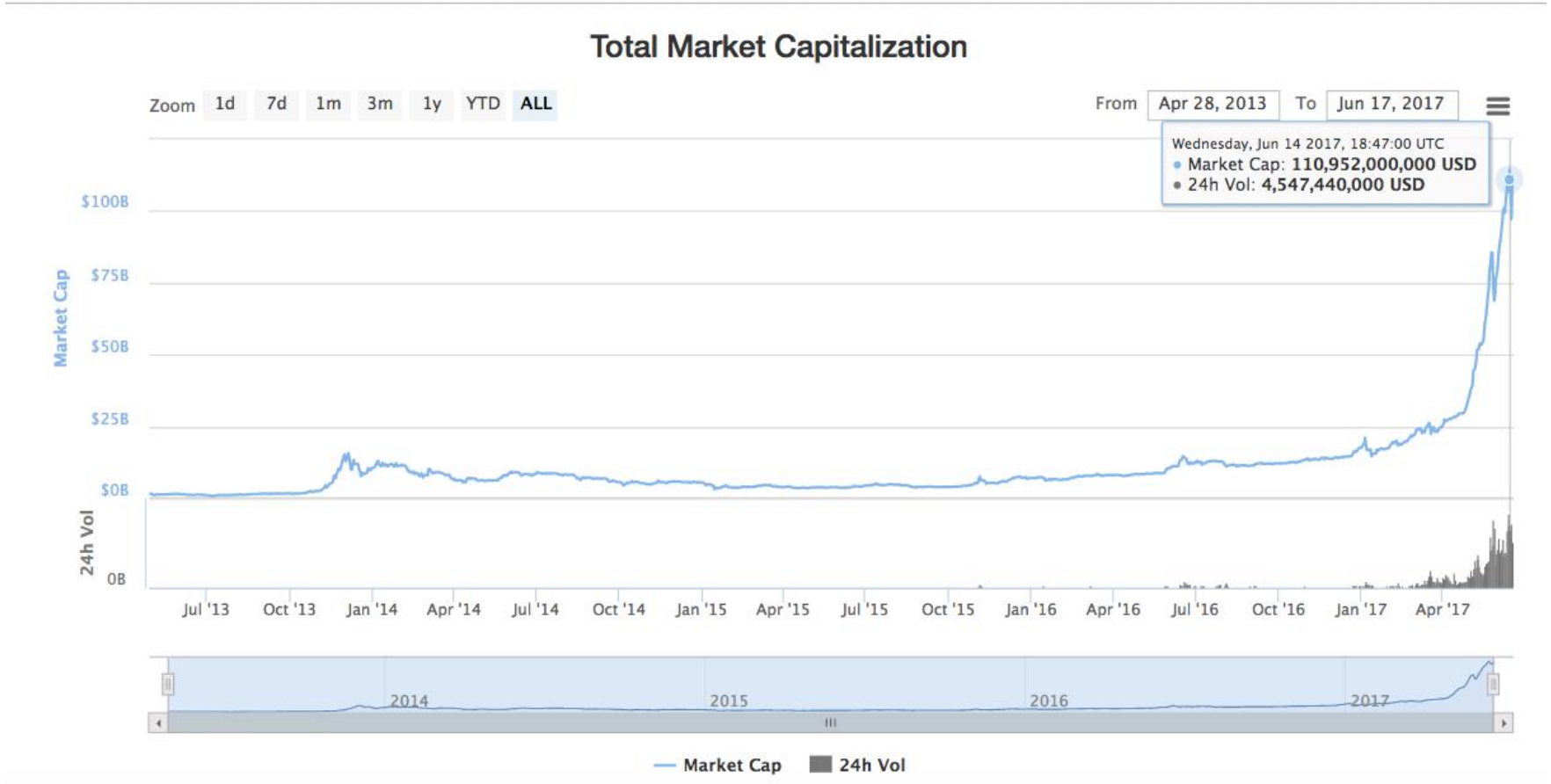
Bitcoin's legal position in Japan is slowly—but surely—becoming clear.

After regulating digital currency exchanges in the country last year, the Japanese Diet has signed a landmark bill that will allow the use of digital currencies like bitcoin as a legal method of payment.

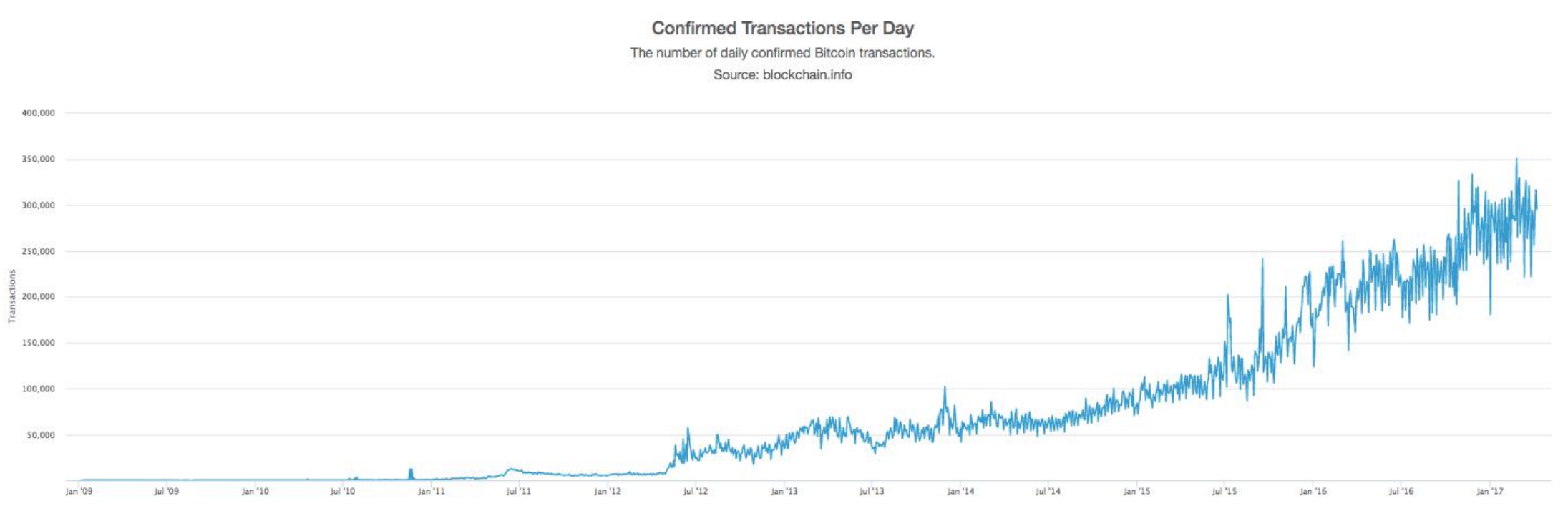
The long-awaited bill, which goes into effect on April 1, still does not recognize bitcoin as a currency, but it has accepted that bitcoin and other cryptocurrencies have "asset-like values" that can be used "as payment to indefinite parties for the cost of purchase or rent of items or receipt of services and which can be transferred by means of electronic data processing systems," **explained** Bitflyer exchange.

"Bitcoin will continue to be treated as an asset unless there are future revisions or directives to Japanese tax law," the exchange noted.

Digital,Currency



# Transactions




DigitalCurrency
Blockchain

The,White,Paper

# Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

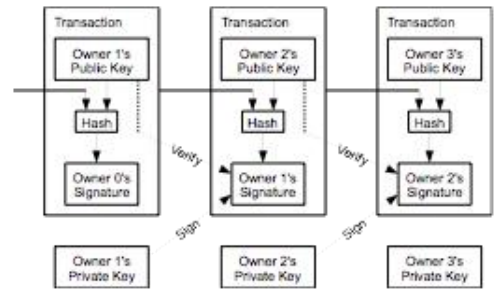
## 1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

## 2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

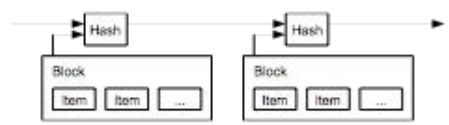


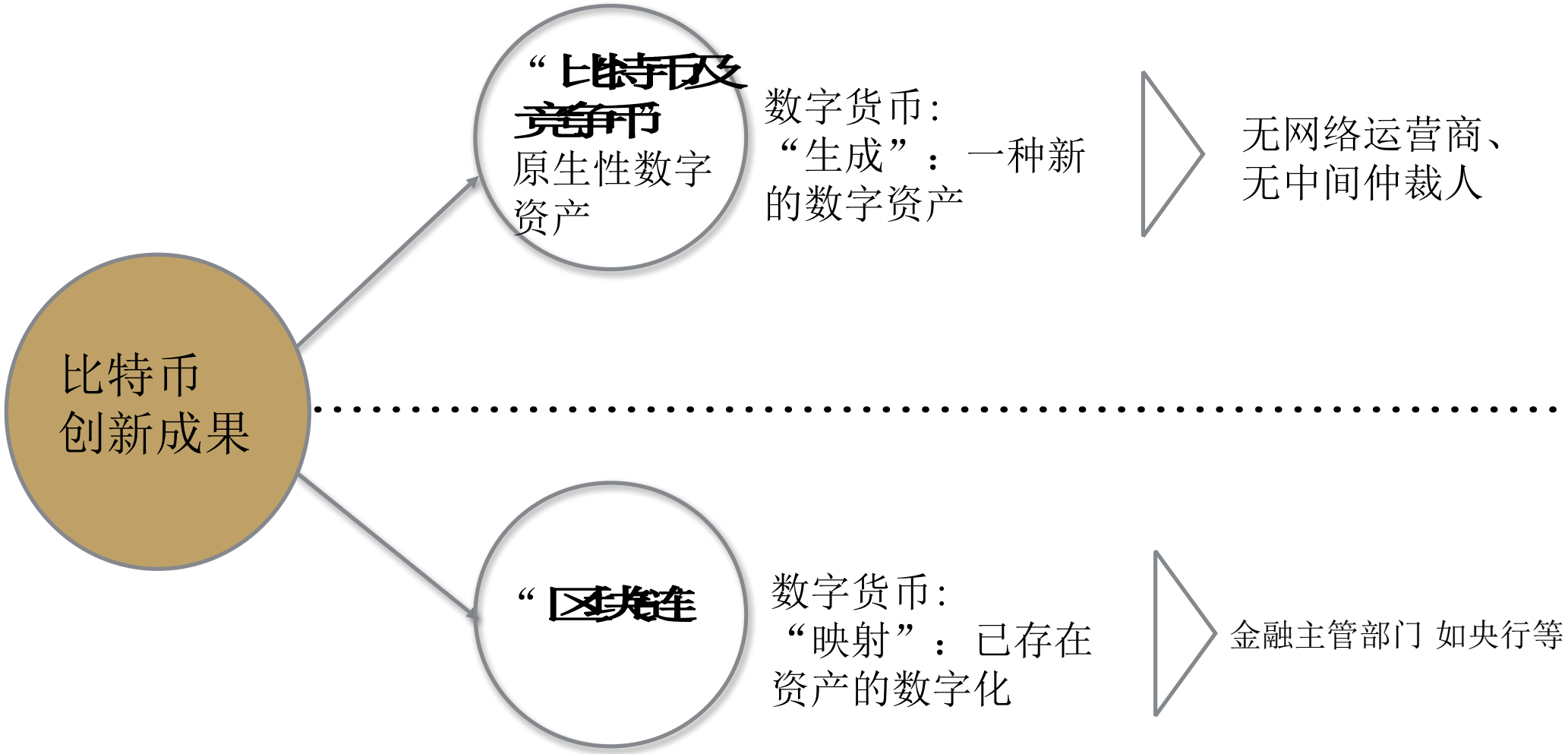

The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

## 3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.




比特币
创新成果
“比特币及竞争币”
原生性数字资产
数字货币：
“生成”：一种新的数字资产
无网络运营商、
无中间仲裁人
“区块链”
数字货币：
“映射”：已存在资产的数字化
金融主管部门 如央行等

BYTOM

# The Internet-Intranet Comparison

**We believe both public and enterprise blockchains have useful applications, much like the Internet and corporate intranets**

## PUBLIC BLOCKCHAINS

public (inter-)
**The internet**

Google amazon

## ENTERPRISE BLOCKCHAINS

ripple Chain HYPERLEDGER

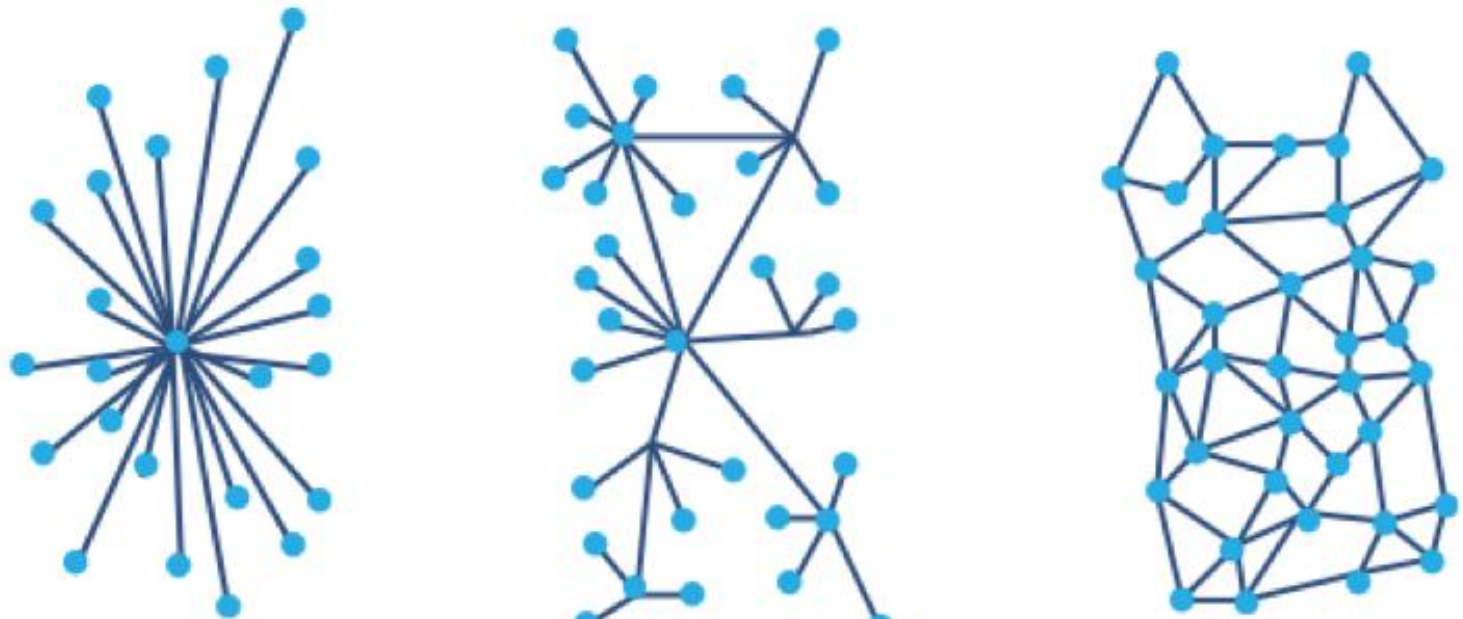
private (intra-)
**Intranets & IT**

ORACLE IBM

# What is the blockchain

BYTOM

A block is created when multiple nodes agree and validate the transactions. “Distributed ledger” comes from the fact that there is no need for a centralized party to validate a transaction.



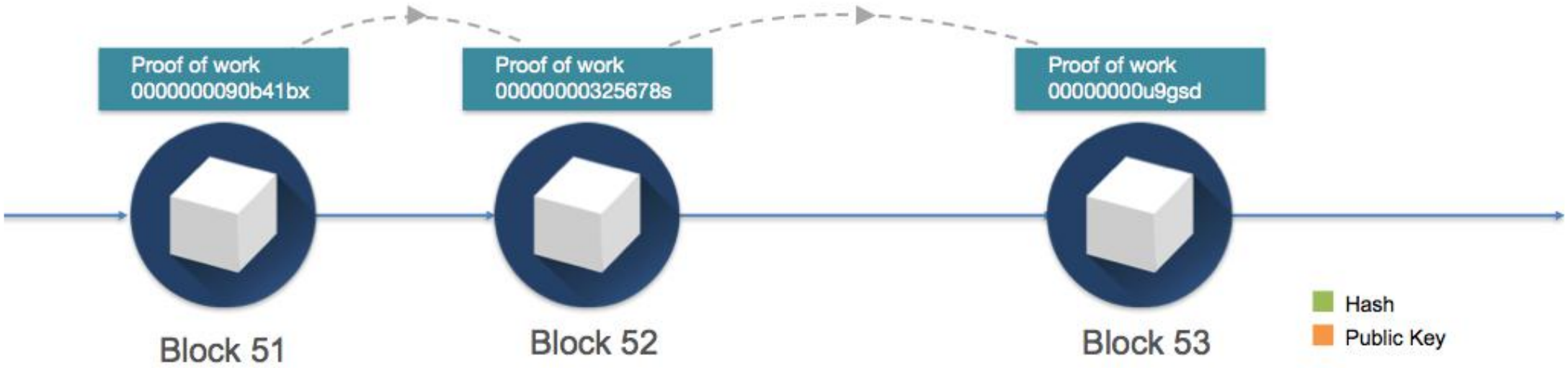

Most secure distributed ledger consensus mechanism:

PROOF OF WORK (PoW) – An economic measure to deter ledger hacking by requiring work from the service requester, usually in the form of computer power over a period of time.

# How blockchain transactions work

BYTOM

Blockchains solve two major challenges for digital transactions, controlling the information and avoiding duplication.




| Transactions |
|---|
| 0000009857w |
| 000000432qrza1 |
| … |

| Transactions |
|---|
| 000000zzxczx |
| 0000009867vw1 |
| … |

| Transactions | Sender | Receiver |
|---|---|---|
| 00000090b41w | 000000jj93xq | 000000x5vw |
| 000000zzxcza1 | 00000090b41 | 00000049bx |
| … | … | … |

- ID referred to as a “hash” called “proof of work.” This is a random set of encrypted digits.
- Transactions numbering from one to many thousands are included in each block.
- Public key identifies the sender and receiver

# Flow of a transaction on the blockchain

BYTOM

- Counterparty A sends funds to Counterparty B

- The transaction is configured into a block

- The transaction is broadcast across the entire network which validates it

- Counterparty B receives funds from Counterparty A

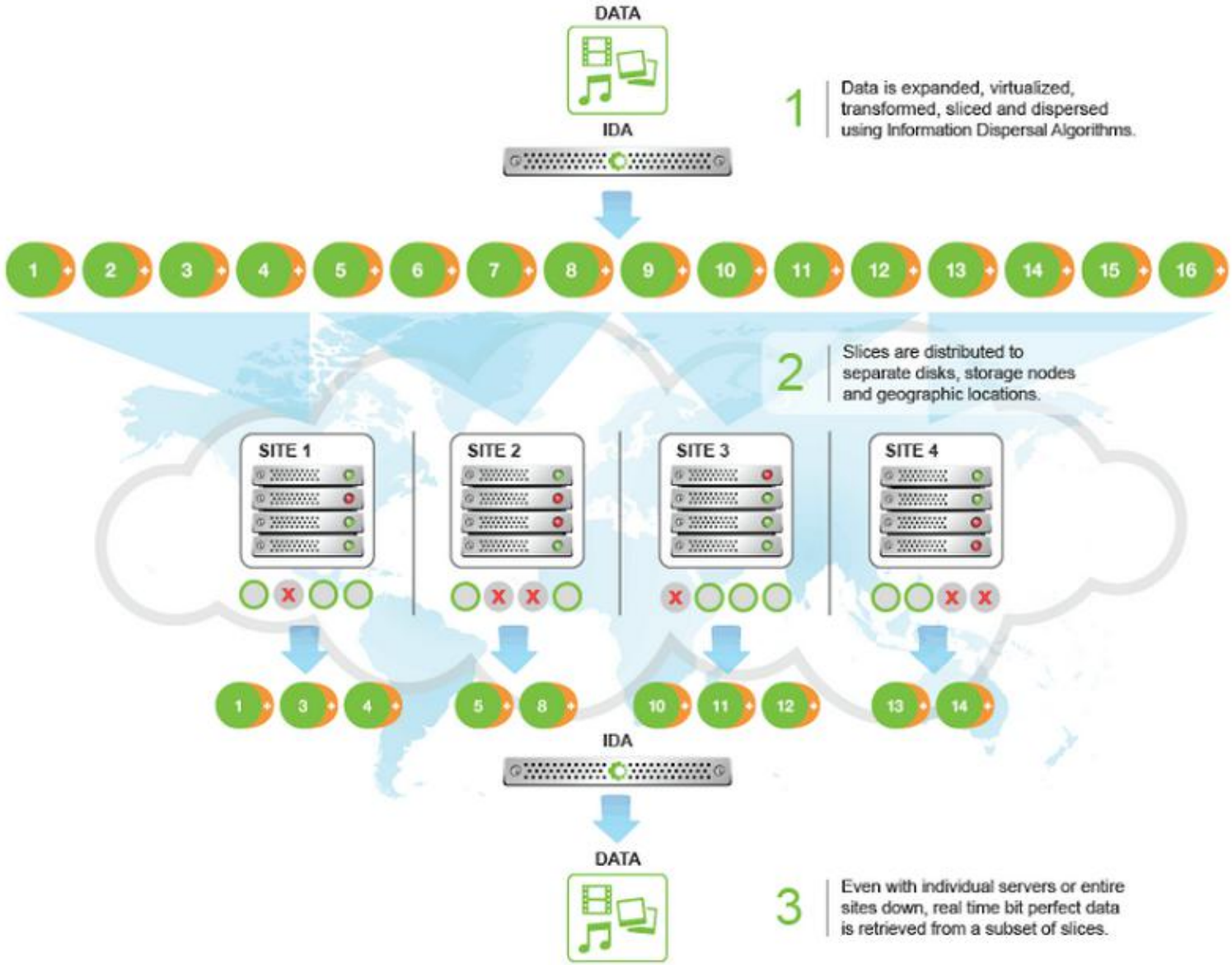
- The block is then added to the chain which records the entire non-reversible history of transactions in a public ledger

- 网络上流通的，不再是或正确或错误、廉价的、长短不一、格式杂乱的“信息”，而是需要一定程度加以保护的，稀缺的“资产”。（这里资产为广义，不论是股权、债券、代币、彩票、还是某种有价值的权益证明）

- 而整个网络运作的逻辑也围绕此点展开：加密，签名，验证，交易，确认，读、写、执行合约 等等。整个网络的运作按照一定的规则，有确定时延的运转：包括生成块、链或者其他名称的“账本”或数据记录、全局状态记录。并不断的通过默克尔树剪枝操作摒弃冗余的、错误的、失效的数据。

“不要拿大炮打蚊子”：区块链技术更适宜于资产网络

*–区块链打造定律1 <区块链产品三定律>*


DATA
IDA
1
Data is expanded, virtualized, transformed, sliced and dispersed using Information Dispersal Algorithms.
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
2
Slices are distributed to separate disks, storage nodes and geographic locations.
SITE 1
SITE 2
SITE 3
SITE 4
1 3 4
5 8
10 11 12
13 14
IDA
DATA
3
Even with individual servers or entire sites down, real time bit perfect data is retrieved from a subset of slices.

# “存储” VS “存证”


存储　与资产无关的数据构成区块链系统商业逻辑漏洞明显

存证　对法律证据、合同、遗嘱证明带来了革命性的改变

BYTOM

# 适用于具有多个弱信任、对等的写入权限节点的数据库

*–区块链打造定律2*

- 在使用区块链之前，一般是不存在信任关系或弱信任关系。节点间一般进行资产交互的方式是：信任第三方。然后通过第三方实体进行“资产”属性数据或凭证的“传递”和“交换”操作。

- 区块链产生后，充当的角色有：公共操作记录的数据库、信任的锚定者等。这个数据库需要一群互不信任、或缺乏信任的节点共同协作，按照既定的规则进行“写”的操作。而“读”和 “执行” 的权限则开放给相应权限的参与者。一个适合传统的C/S模型硬性改造成区块链也是毫无意义的。

BYTOM

# 适用于去中心化的解决方案

*–区块链打造定律3*

# 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、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、量子链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

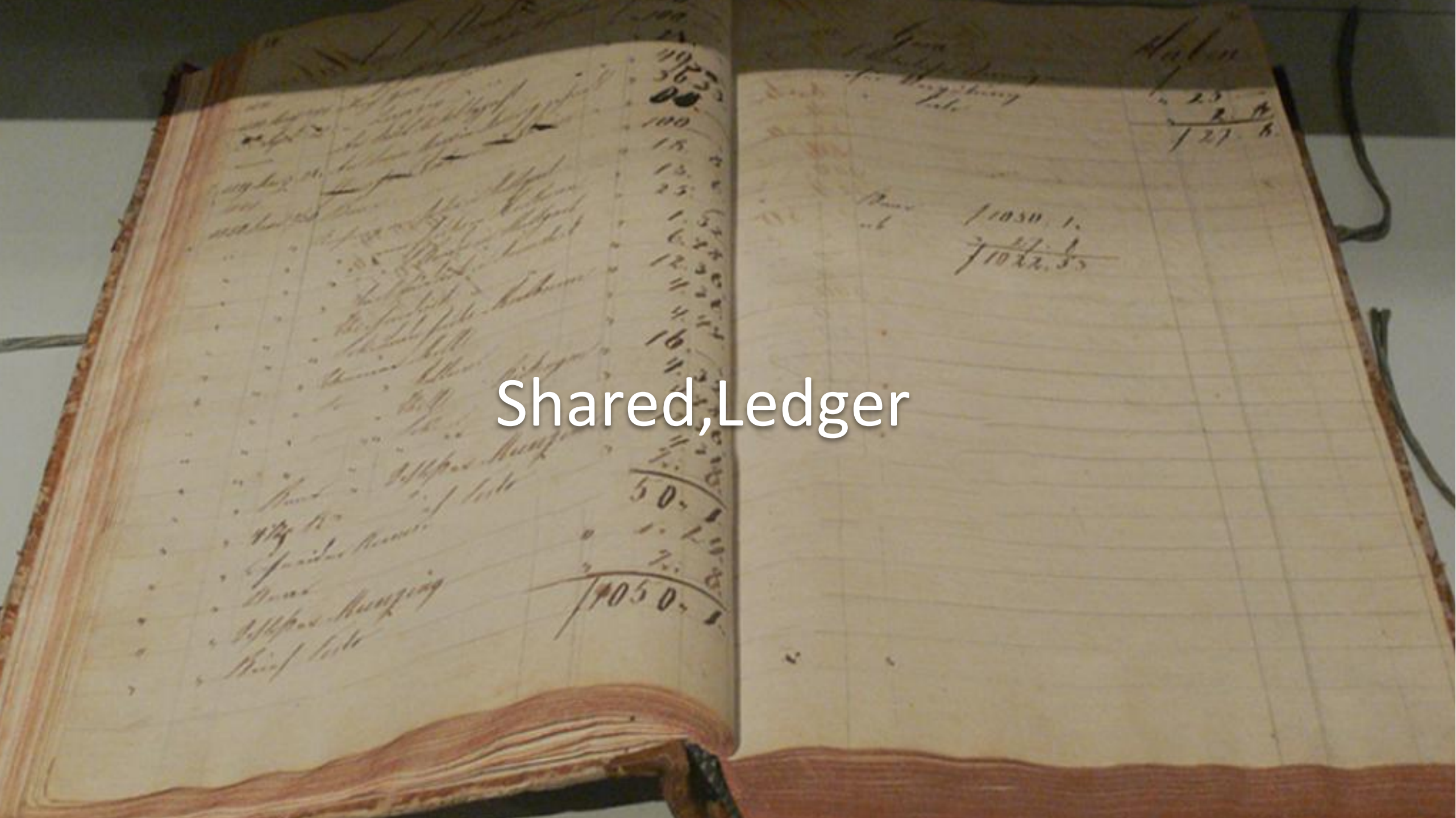
#### 1.3.1 建造多元化比特资产登记的标准

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。

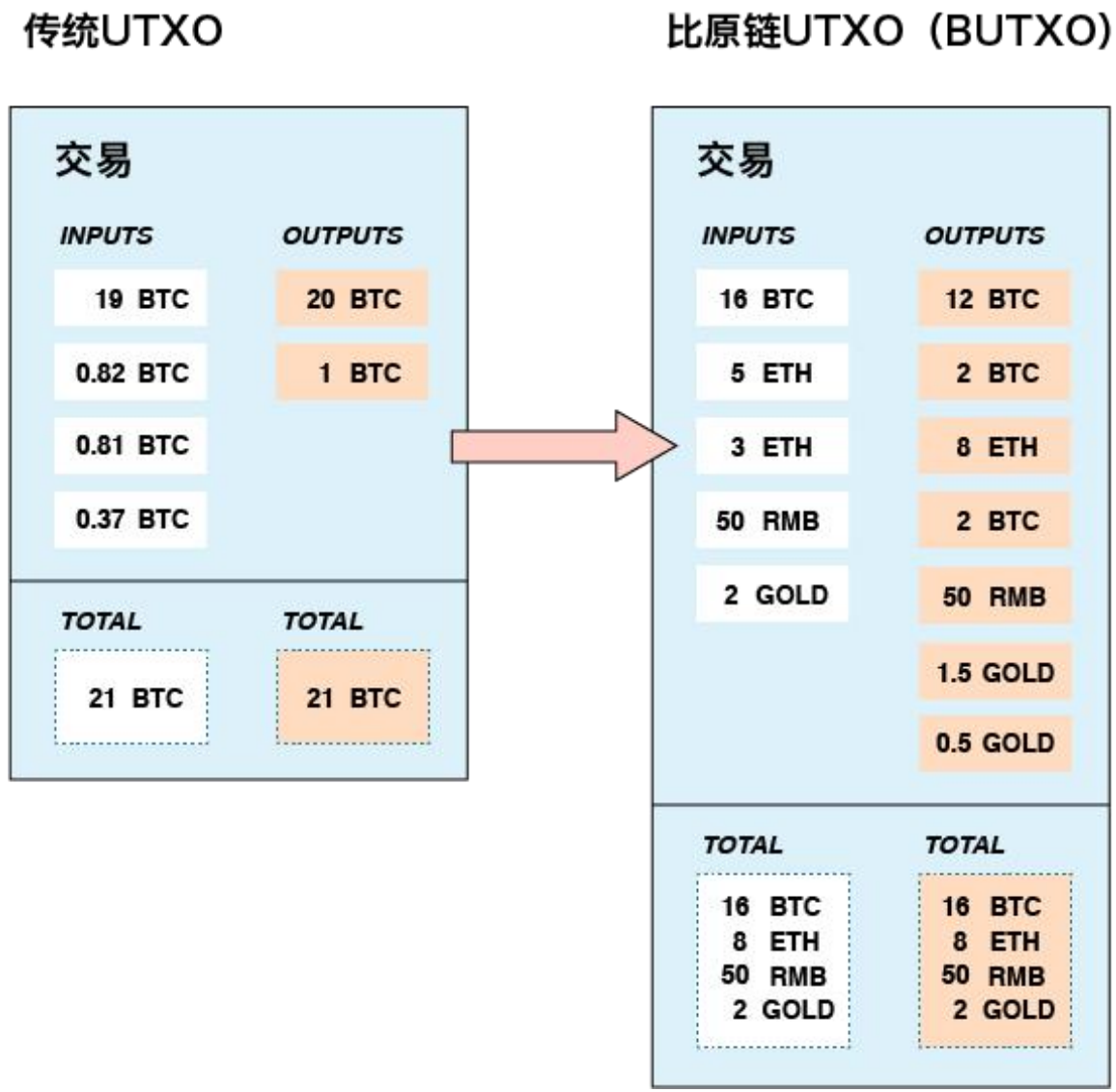
#### 1.3.2 建造多元化比特资产的交互工具

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；

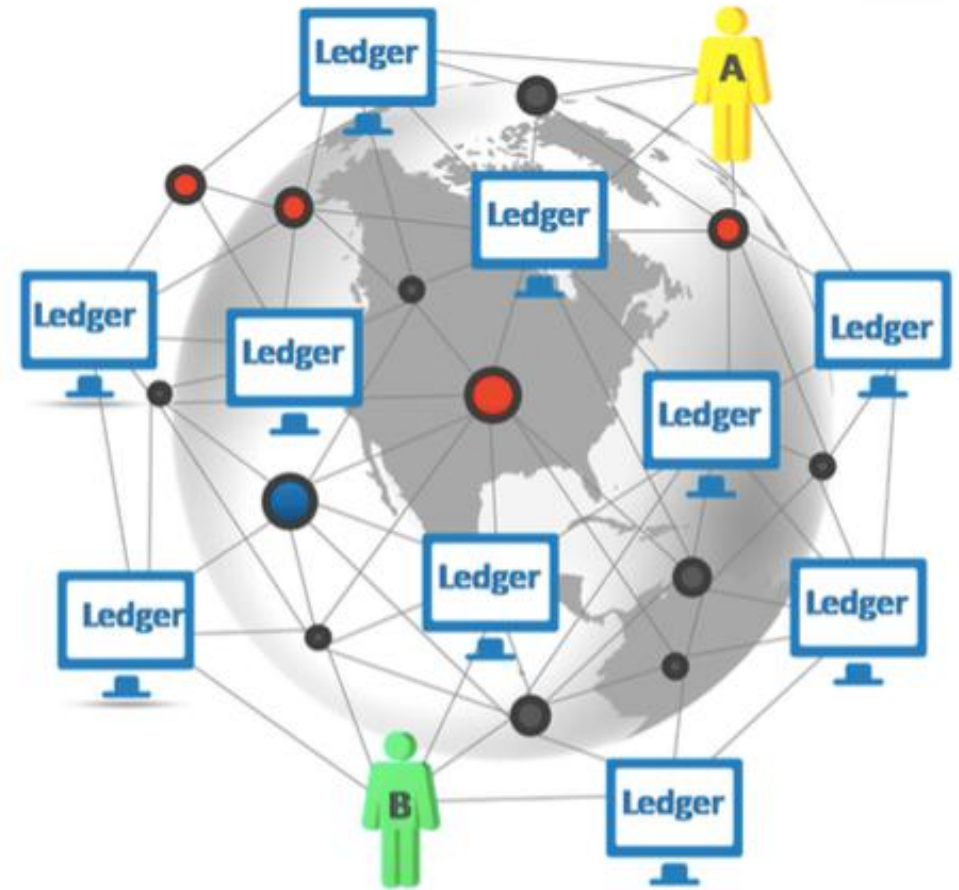

Shared,Ledger

# （一）账本角度的扩展


传统UTXO
交易
INPUTS
OUTPUTS
19 BTC
20 BTC
0.82 BTC
1 BTC
0.81 BTC
0.37 BTC
TOTAL
TOTAL
21 BTC
21 BTC
比原链UTXO（BUTXO）
交易
INPUTS
OUTPUTS
16 BTC
12 BTC
5 ETH
2 BTC
3 ETH
8 ETH
50 RMB
2 BTC
2 GOLD
50 RMB
1.5 GOLD
0.5 GOLD
TOTAL
TOTAL
16 BTC
8 ETH
50 RMB
2 GOLD
16 BTC
8 ETH
50 RMB
2 GOLD

BYTOM

***An illustrative example of distributed ledger system similar to Bitcoin (Blockchain)***




*Payment from A to B:*

- Copies of transaction records (ledgers) are kept in multiple computers in the network and visible to anyone.
- The transaction is settled by a multitude of individual nodes (miners), providing computing resources to the network.
- Miners solve a cryptographic puzzle as part of validation process. Miners need to show proof of doing this work to the network (called a "proof-of-work" system), which is costly (computing and energy resources).
- Only the miner who finds the solution faster than any others receives newly minted Bitcoins as reward for their service.
- "Trust" is created by making tampering attempts prohibitively expensive. If a miner wants to record a false transaction, she needs to compete against other miners who are acting honestly (or trying to fake a different transaction).[1]

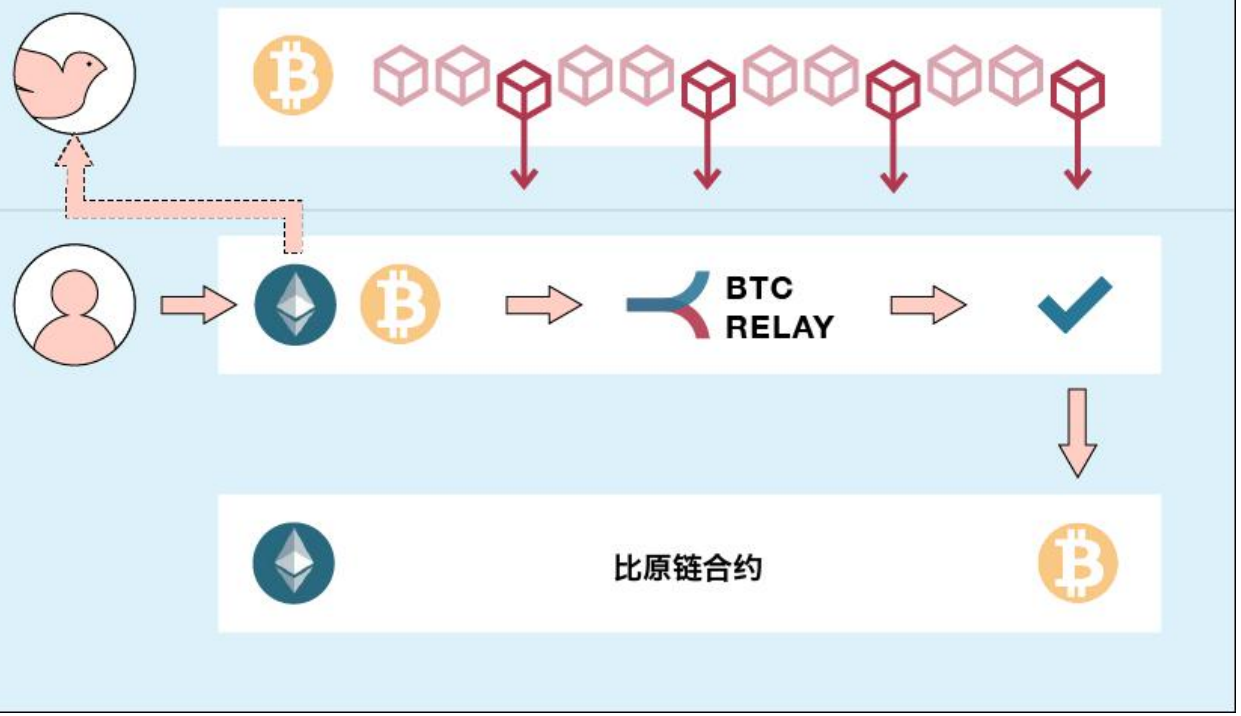

BYTOM

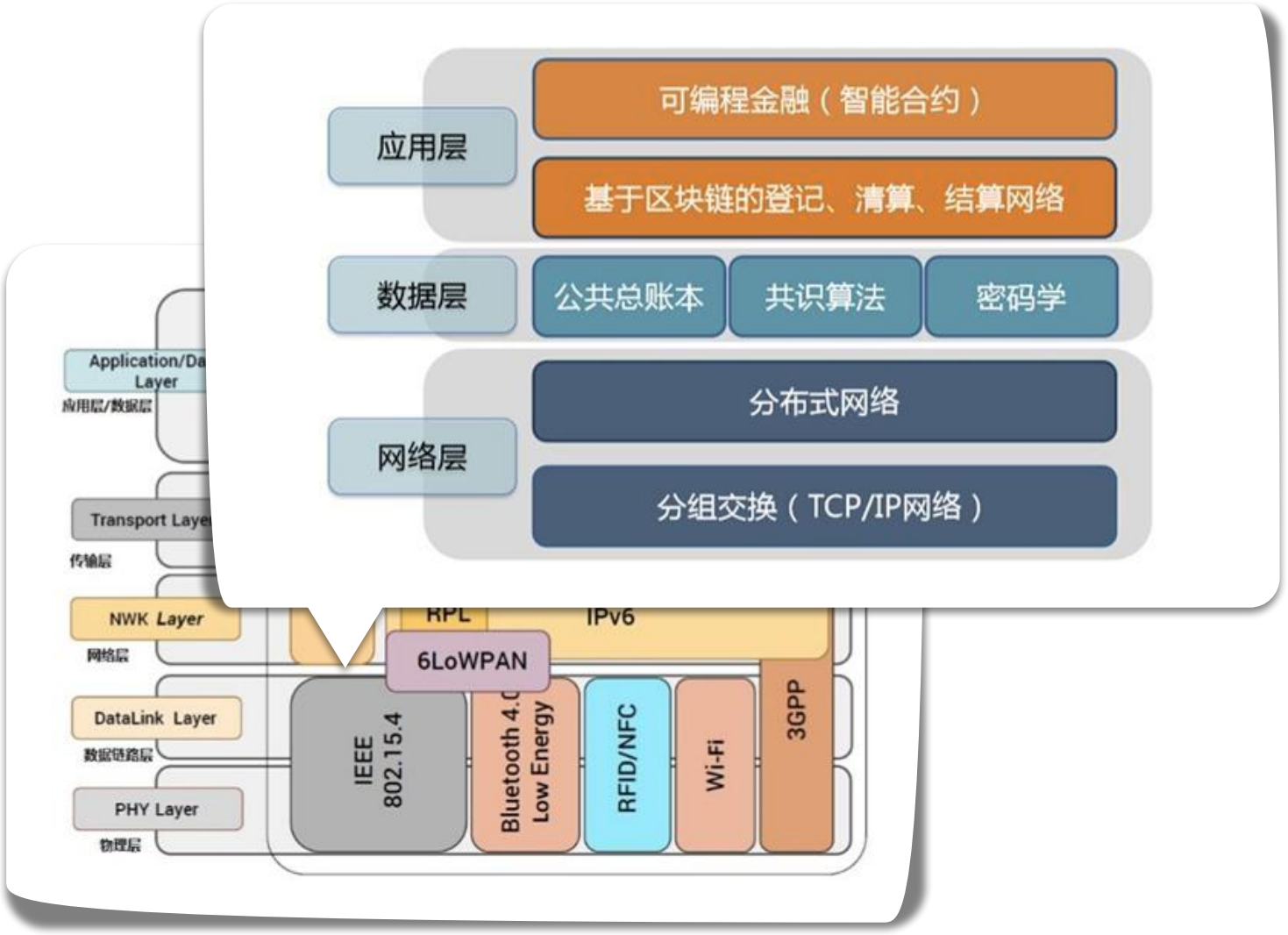
# （二）网络角度的扩展

X Relayers 跨链读取其他链区块信息及状态

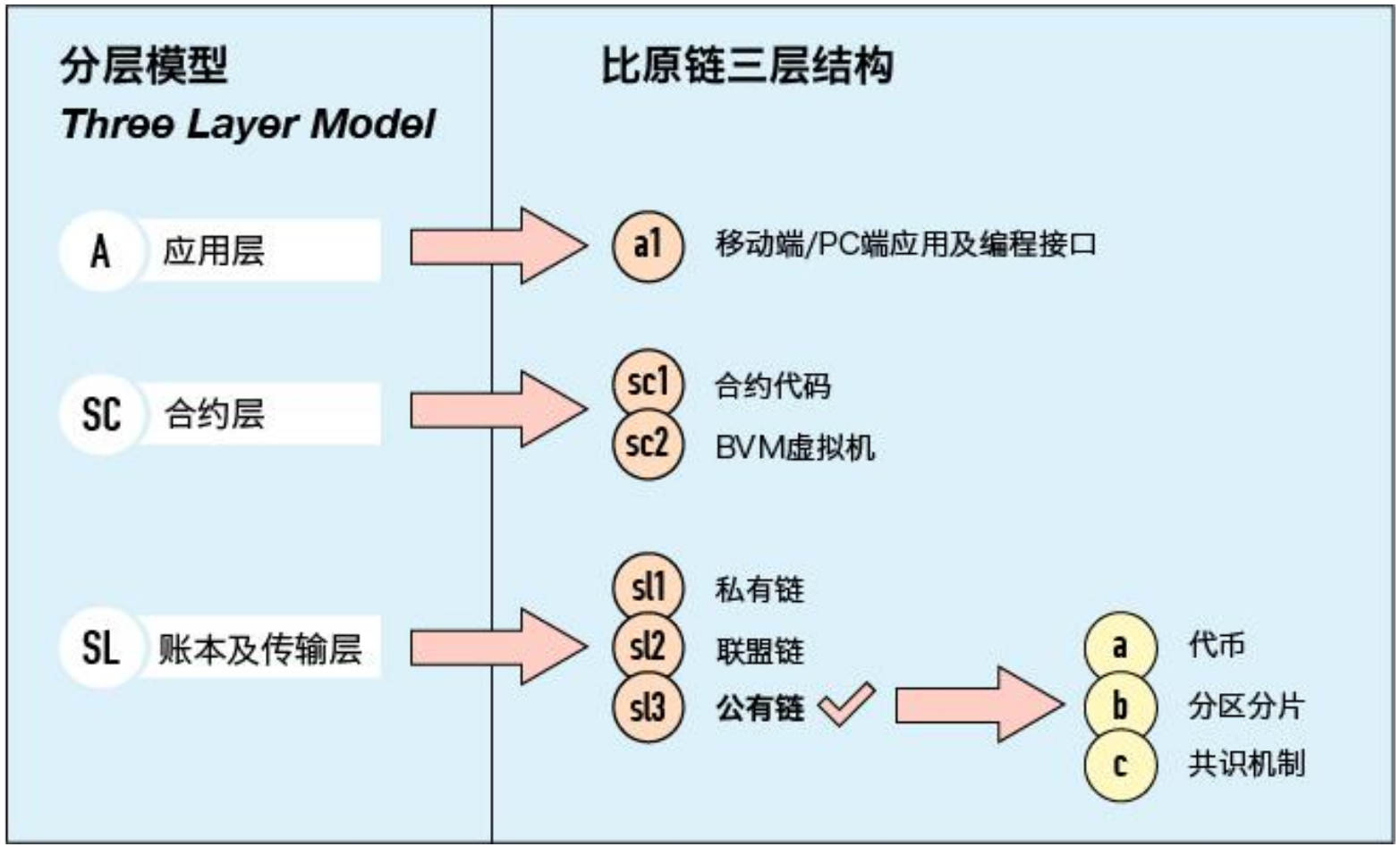
X Relayers 通过支付小额费用嵌入其他链交易中

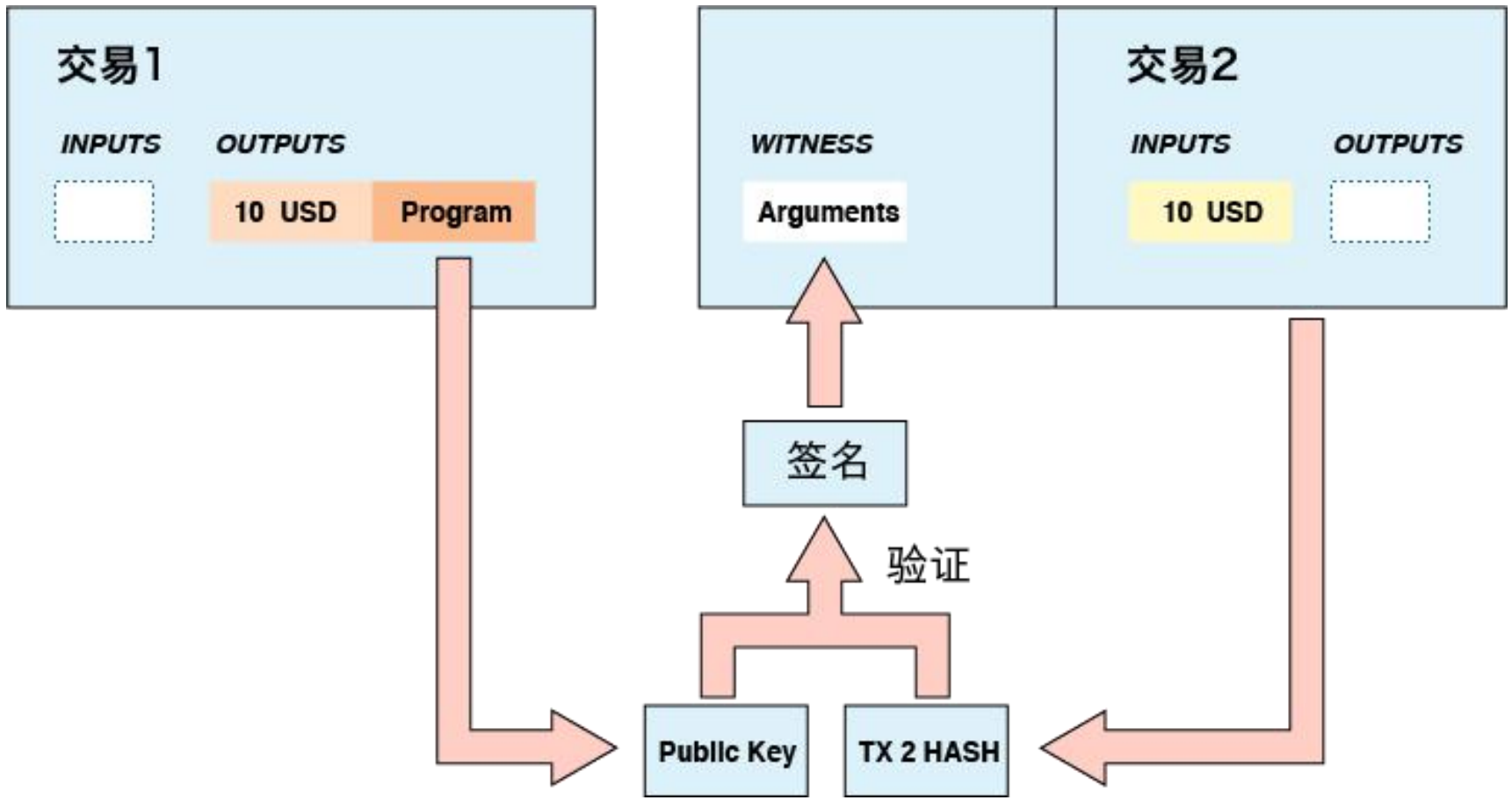
验证过后的交易信息可供此原链上的合约读取




应用层
可编程金融（智能合约）
基于区块链的登记、清算、结算网络
数据层
公共总账本
共识算法
密码学
网络层
分布式网络
分组交换（TCP/IP网络）
Application/Da Layer
应用层/数据层
Transport Laye
传输层
NWK Layer
网络层
DataLink Layer
数据链路层
PHY Layer
物理层
RPL
IPv6
6LoWPAN
IEEE 802.15.4
Bluetooth 4.0 Low Energy
RFID/NFC
Wi-Fi
3GPP

（三）合约层面的改进


分层模型
Three Layer Model
比原链三层结构
A
应用层
a1
移动端/PC端应用及编程接口
SC
合约层
sc1
合约代码
sc2
BVM虚拟机
SL
账本及传输层
sl1
私有链
sl2
联盟链
sl3
公有链
a
代币
b
分区分片
c
共识机制


交易1
INPUTS
OUTPUTS
10 USD
Program
WITNESS
Arguments
交易2
INPUTS
OUTPUTS
10 USD
签名
验证
Public Key
TX 2 HASH

BYTOM

## UTXO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。

## 通用地址格式

比原链钱包将引入BIP32，BIP43，BIP44理念。

## 支持国密标准

比原链由三层组成，数据交易及传输层、合约层、资产交互层。

## 对人工智能ASIC友好

在比原链共识机制中引入了新型POW算法。


## 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。

## 数据与签名分离

设计了一种多种资产可以互相交易发布的分布式账本协议。

## 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。

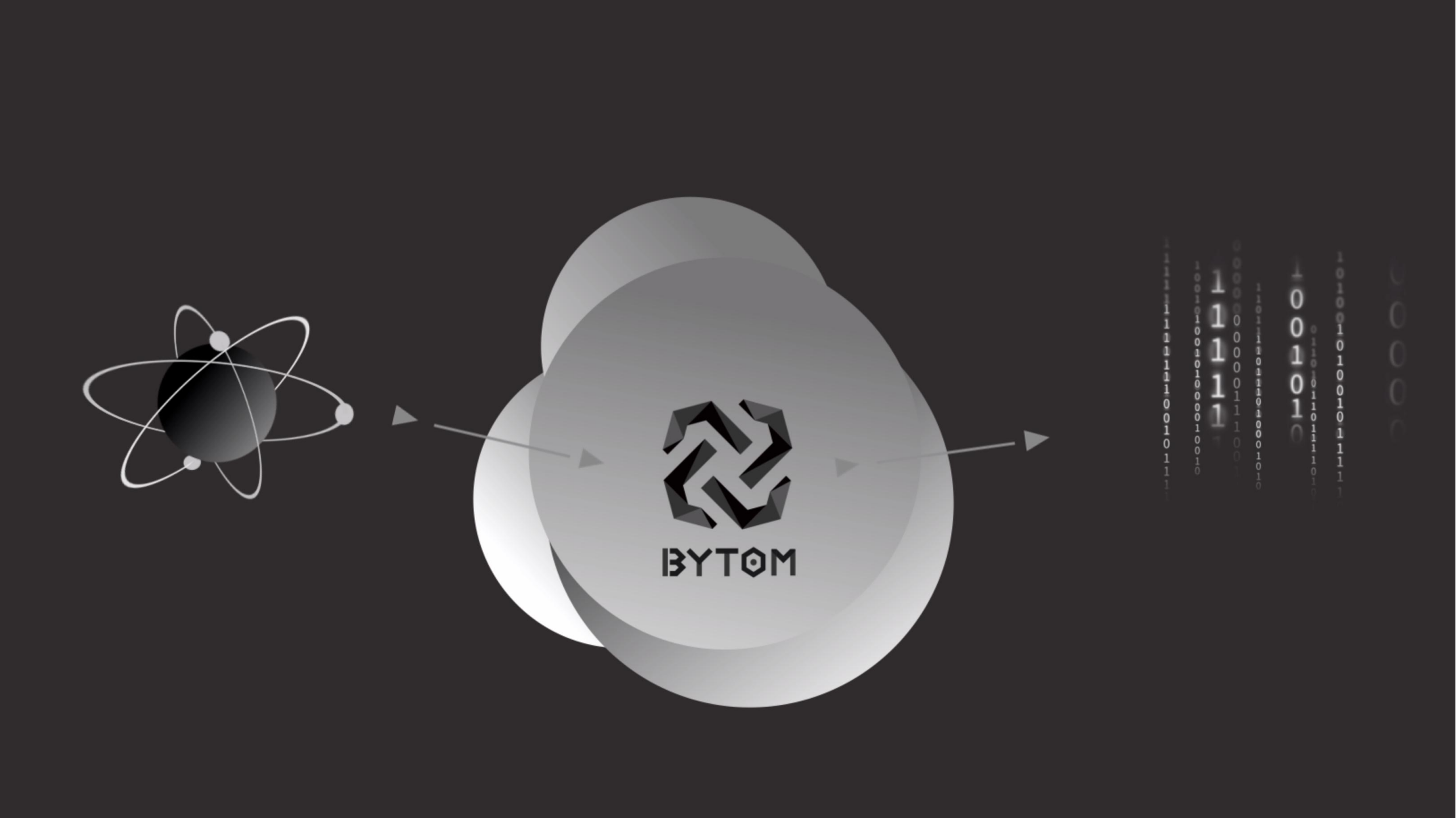
## 基于侧链的跨链分红

开发者可以在比原链上创建一种小型版本的X链。

文字

物理载体


数字载体


BYTOM

# Contact us
# 联系我们

比原链官方网站

http://bytom.io

段新星

WechatID:CSCEC-YNYA