China Blockchain Conference

区块链中的进阶密码学

徐海霞
xuhaixia@iie.ac.cn

中国科学院信息工程研究所

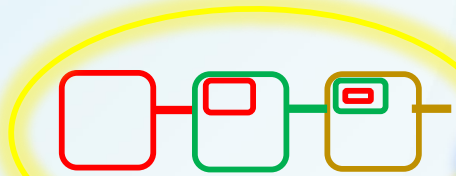
China Blockchain Conference

目录

China Blockchain Conference

目录

区块链是什么



微观上数据存储在块中，块在逻辑上串联构成链条

区块链(Blockchain)

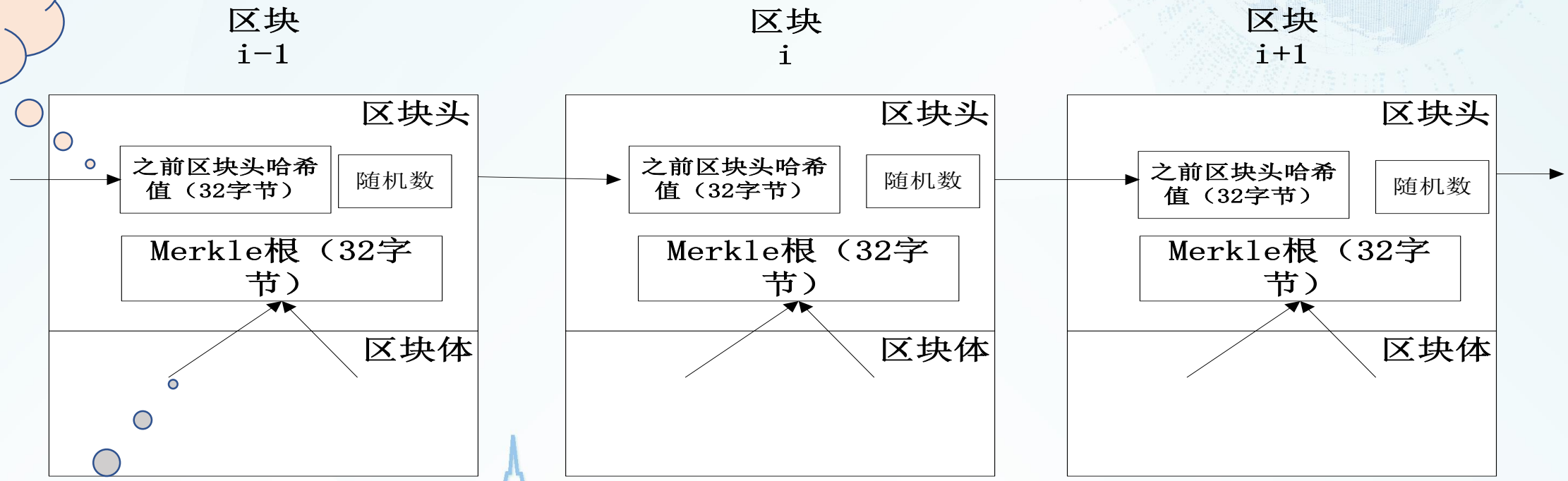
- 是一种分布式交易验证和数据共享技术
- 也被称为分布式共享总账

特点：

- 分布式平等部署系统
- 分布式共享相同数据
- 无中心控制
- 全网节点协作完成交易验证存储

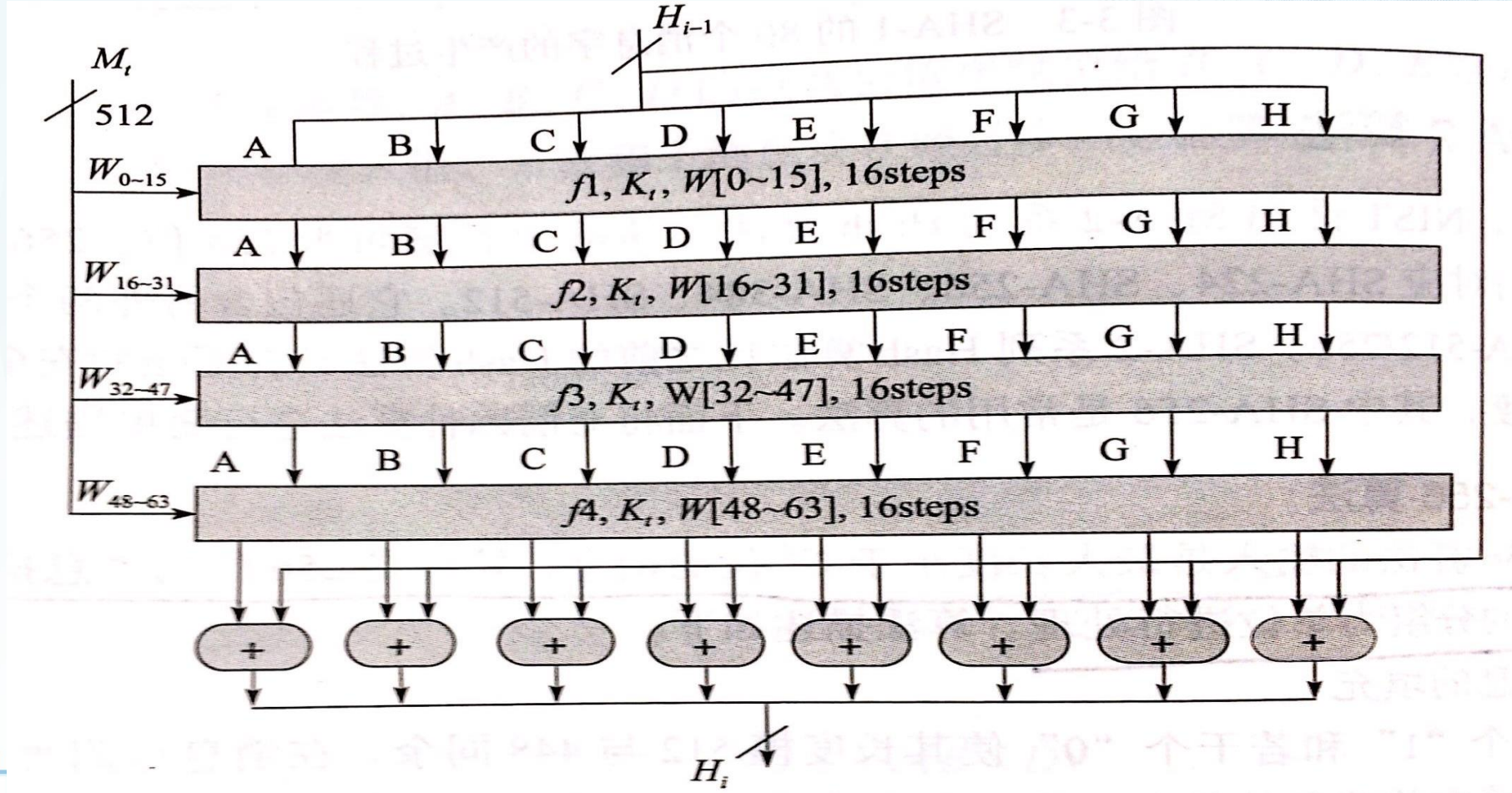
Hash函数

Hash chain of blocks

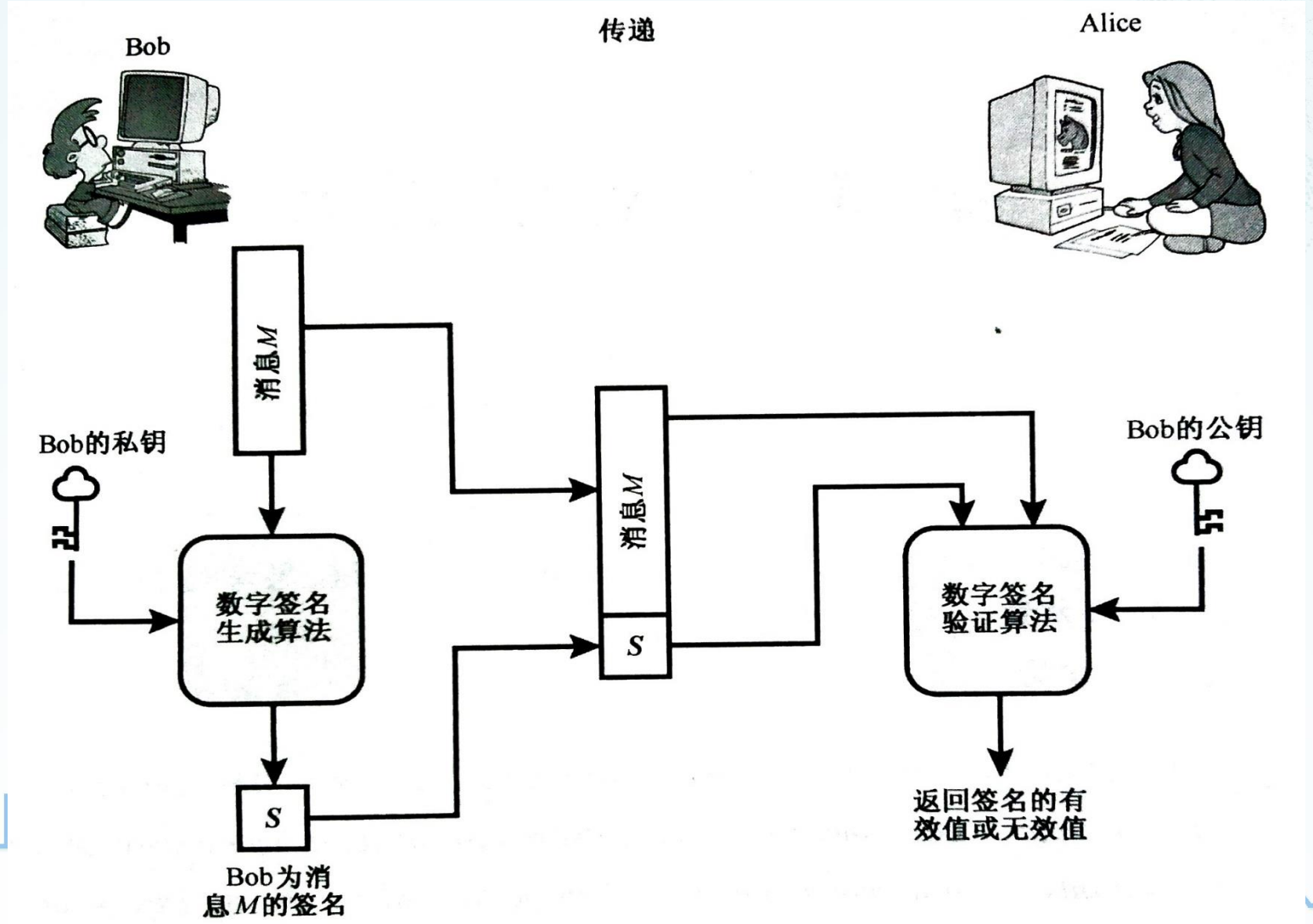


Hash tree of transactions

SHA-256


H_{i-1}
M_t
512
A B C D E F G H
$W_{0\sim15}$
$f1, K_t, W[0\sim15]$, 16steps
A B C D E F G H
$W_{16\sim31}$
$f2, K_t, W[16\sim31]$, 16steps
A B C D E F G H
$W_{32\sim47}$
$f3, K_t, W[32\sim47]$, 16steps
A B C D E F G H
$W_{48\sim63}$
$f4, K_t, W[48\sim63]$, 16steps
+ + + + + + + +
H_i

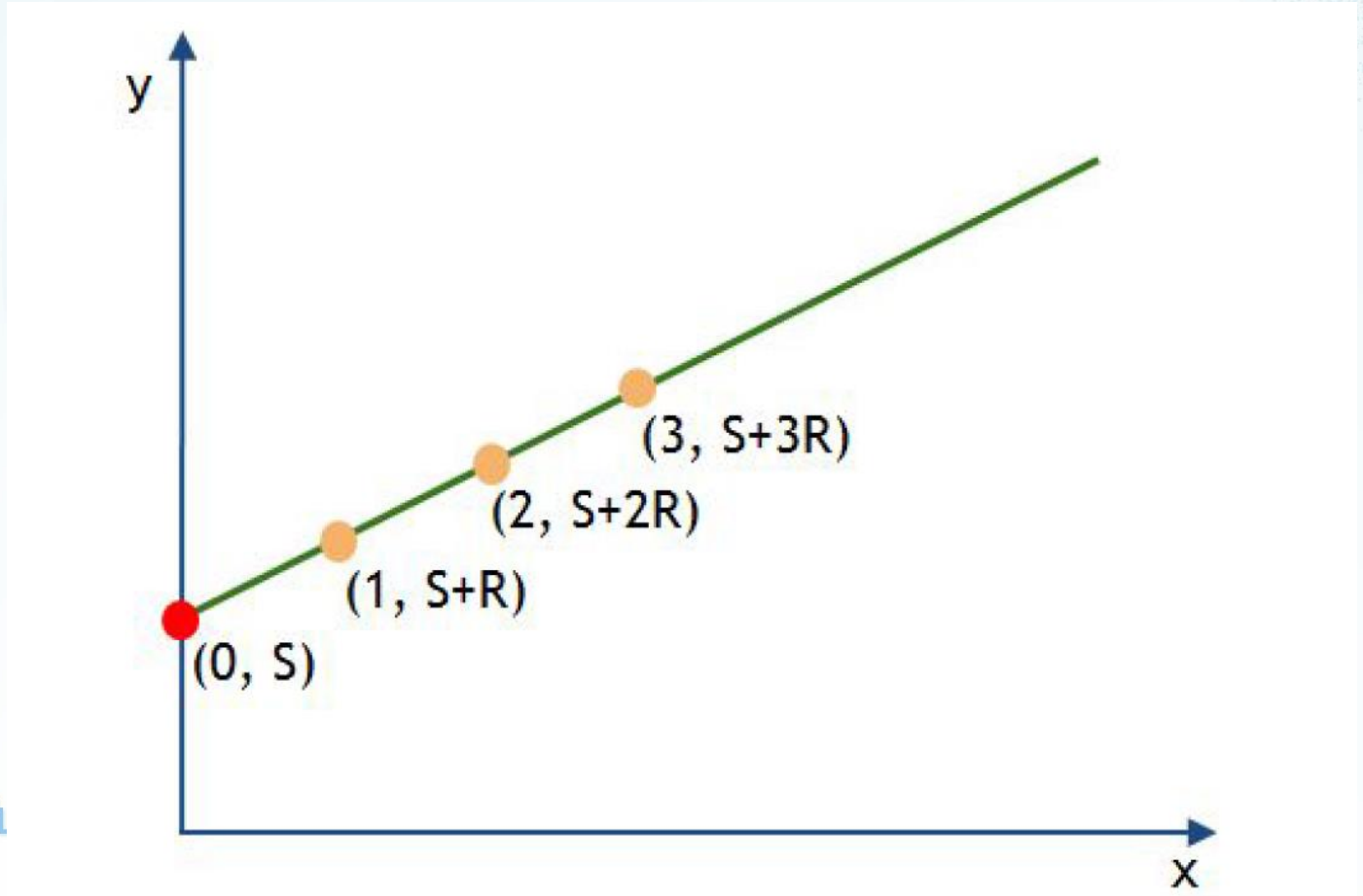
Signature


Bob
传递
Alice
消息M
Bob的私钥
Bob的公钥
数字签名
生成算法
消息M
S
数字签名
验证算法
S
返回签名的有
效值或无效值
Bob为消
息M的签名

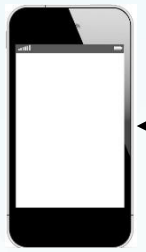
Hierarchical wallets

- Private key : k, x, y
- ith sk: $x_i = y + H(k||i)$
- Address : k, g^y
- ith pk: $g^{x_i} = g^{H(k||i)} g^y$
- ith address: $H(g^{x_i})$

(n,2) Secret sharing



Threshold Signature



双方合作签名

(sk_1, r_1)

(sk_2, r_2)

China Blockchain Conference

目录

效率

币种	吞吐量（TPS）
比特币	7
Hyperledger Fabric 1.0	1,000
VISA	56,000
支付宝双11	256,000
微信除夕红包	760,000

安全

- 安全性证明&形式化验证
- 应急预案
- 钱包、交易所攻击
- 量子计算机

隐私

- 敏感信息(账户、余额等)
- 数据公开存储

China Blockchain Conference

基础 进阶 挑战

工作量证明

Bitcoin

Bitcoin-NG

PoUW

Fruit

工作量证明+
拜占庭容错协议

Elastico

权益证明

nextcoin

Iching

工作量证明+
权益证明

PPcoin

PoA

2-hop

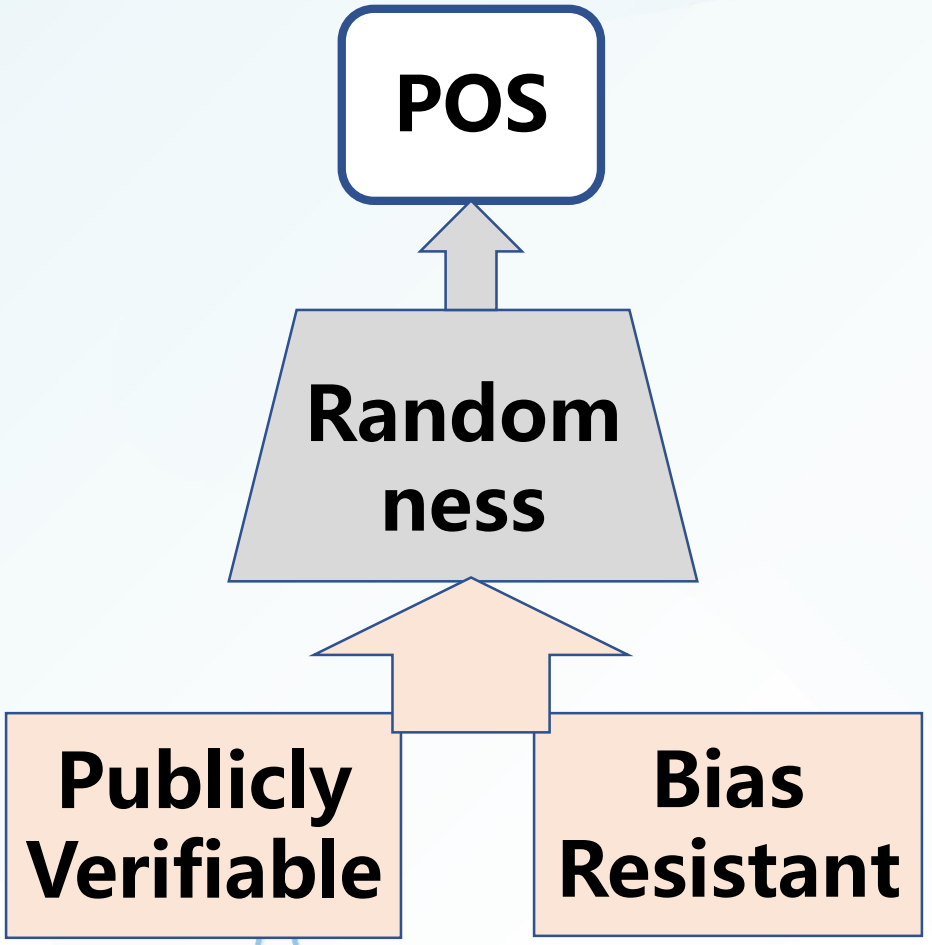
权益证明+
拜占庭容错协议
/安全多方计算

Algorand

Ouroboros

Snowwhite

2008 2012 2013 2014 2016 2017 2018


POS
Randomness
Publicly Verifiable
Bias Resistant

	Signature	VRF	PVSS
Dfinity	✓		
Algorand		✓	
Ouroborus			✓
Scrape			Optimized
Randherd			✓

Coin-tossing into the well

$$(1^n, 1^n) \longrightarrow (b, b)$$

where b is uniformly distributed in $\{0, 1\}$.

A Coin-tossing-into-the-well Protocol

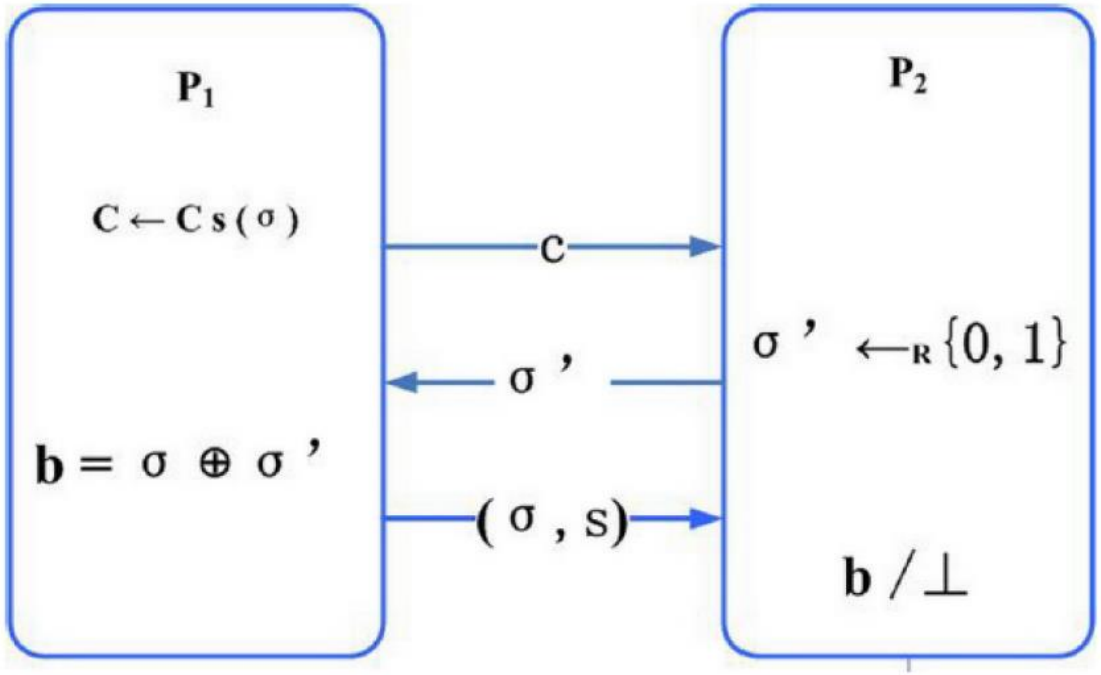
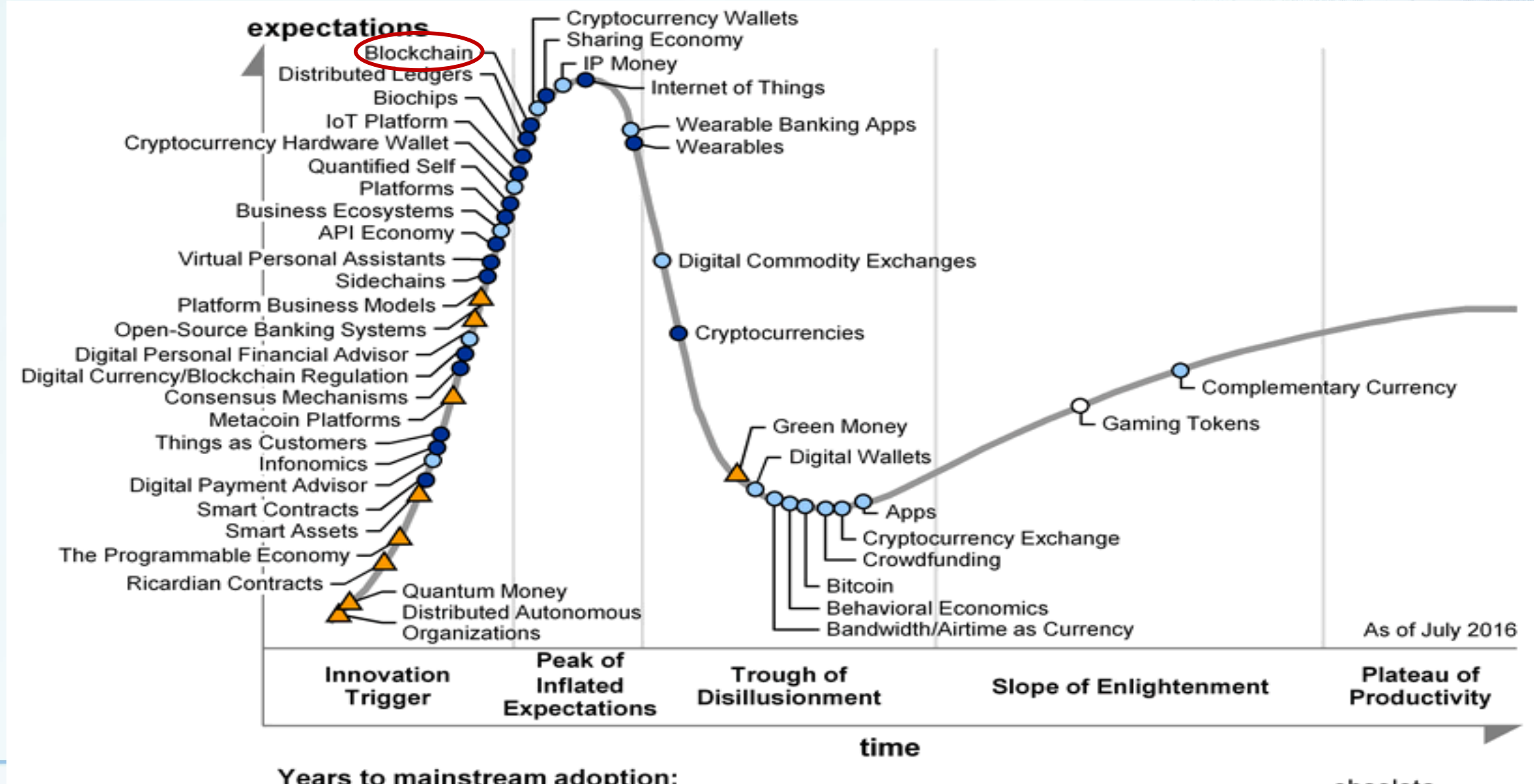
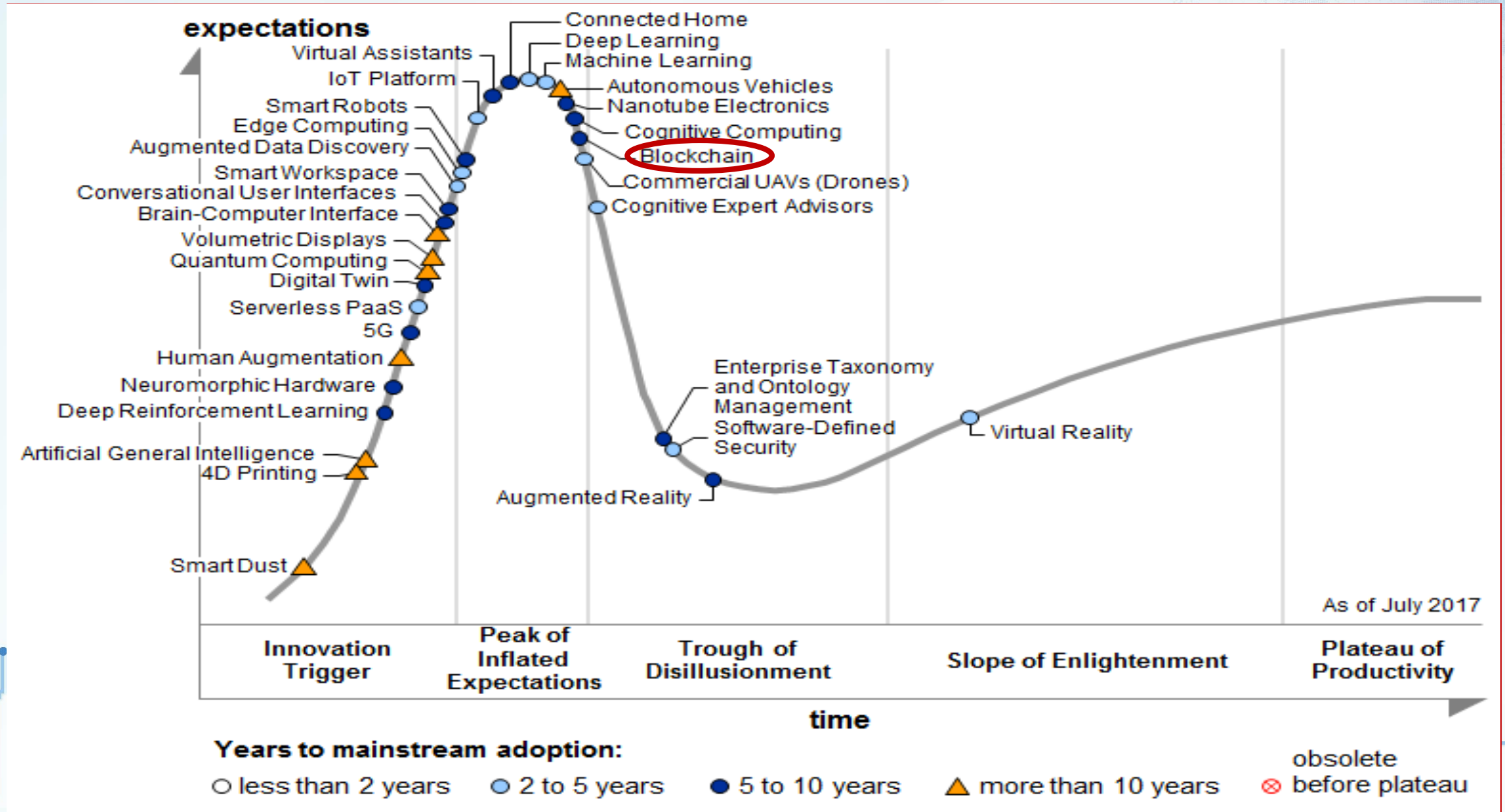
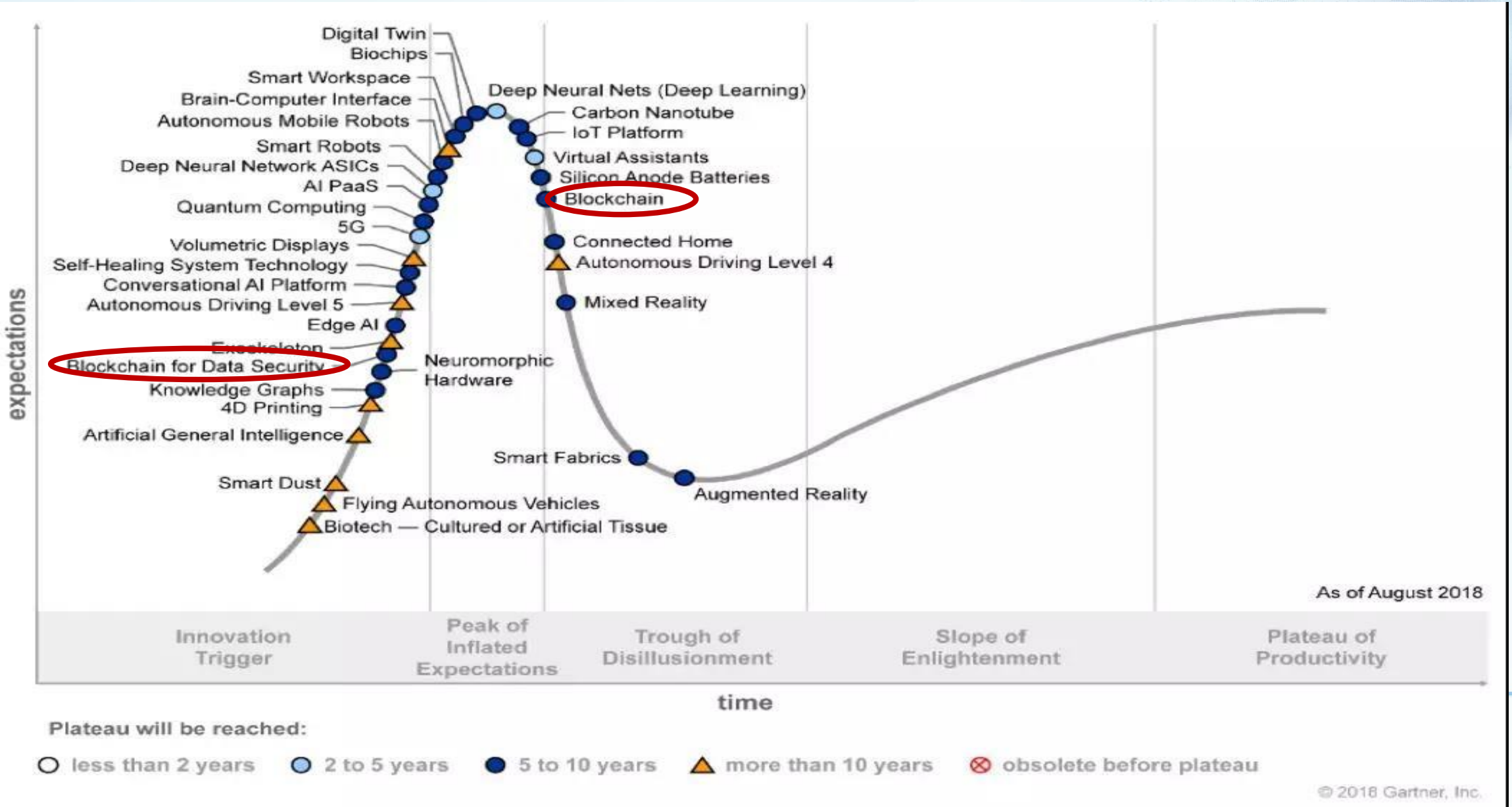


Figure: Coin Tossing Protocol


expectations
Blockchain
Distributed Ledgers
Biochips
IoT Platform
Cryptocurrency Hardware Wallet
Quantified Self
Platforms
Business Ecosystems
API Economy
Virtual Personal Assistants
Sidechains
Platform Business Models
Open-Source Banking Systems
Digital Personal Financial Advisor
Digital Currency/Blockchain Regulation
Consensus Mechanisms
Metacoin Platforms
Things as Customers
Infonomics
Digital Payment Advisor
Smart Contracts
Smart Assets
The Programmable Economy
Ricardian Contracts
Quantum Money
Distributed Autonomous Organizations
Cryptocurrency Wallets
Sharing Economy
IP Money
Internet of Things
Wearable Banking Apps
Wearables
Digital Commodity Exchanges
Cryptocurrencies
Green Money
Digital Wallets
Apps
Cryptocurrency Exchange
Crowdfunding
Bitcoin
Behavioral Economics
Bandwidth/Airtime as Currency
Complementary Currency
Gaming Tokens
As of July 2016
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
time
Years to mainstream adoption:
less than 2 years
2 to 5 years
5 to 10 years
more than 10 years
obsolete before plateau


expectations
Connected Home
Deep Learning
Machine Learning
Virtual Assistants
IoT Platform
Autonomous Vehicles
Nanotube Electronics
Smart Robots
Edge Computing
Cognitive Computing
Augmented Data Discovery
Blockchain
Smart Workspace
Commercial UAVs (Drones)
Conversational User Interfaces
Cognitive Expert Advisors
Brain-Computer Interface
Volumetric Displays
Quantum Computing
Digital Twin
Serverless PaaS
5G
Human Augmentation
Enterprise Taxonomy and Ontology Management
Neuromorphic Hardware
Software-Defined Security
Deep Reinforcement Learning
Virtual Reality
Artificial General Intelligence
4D Printing
Augmented Reality
Smart Dust
As of July 2017
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
time
Years to mainstream adoption:
less than 2 years
2 to 5 years
5 to 10 years
more than 10 years
obsolete before plateau


Digital Twin
Biochips
Smart Workspace
Brain-Computer Interface
Autonomous Mobile Robots
Smart Robots
Deep Neural Network ASICs
AI PaaS
Quantum Computing
5G
Volumetric Displays
Self-Healing System Technology
Conversational AI Platform
Autonomous Driving Level 5
Edge AI
Exoskeleton
Blockchain for Data Security
Knowledge Graphs
4D Printing
Artificial General Intelligence
Smart Dust
Flying Autonomous Vehicles
Biotech — Cultured or Artificial Tissue
Neuromorphic Hardware
Deep Neural Nets (Deep Learning)
Carbon Nanotube
IoT Platform
Virtual Assistants
Silicon Anode Batteries
Blockchain
Connected Home
Autonomous Driving Level 4
Mixed Reality
Smart Fabrics
Augmented Reality
expectations
As of August 2018
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
time
Plateau will be reached:
less than 2 years
2 to 5 years
5 to 10 years
more than 10 years
obsolete before plateau
© 2018 Gartner, Inc.

方案	发送方隐私	接收方隐私	隐藏交易金额	技术
Zerocoin	√	×	×	NIZK&Accumulator
Zerocash	√	√	√	ZK-SNARK
RingCT2.0	√	√	√	NIZK&Accumulator
DASH	√	×	×	Mixing
Monero	√	√	√	Ring Signatures
Zcash	√	√	√	ZK-SNARK

环签名（Ring Signature）

2001年，Rivest, shamir和Tauman三位密码学家首次提出了环签名

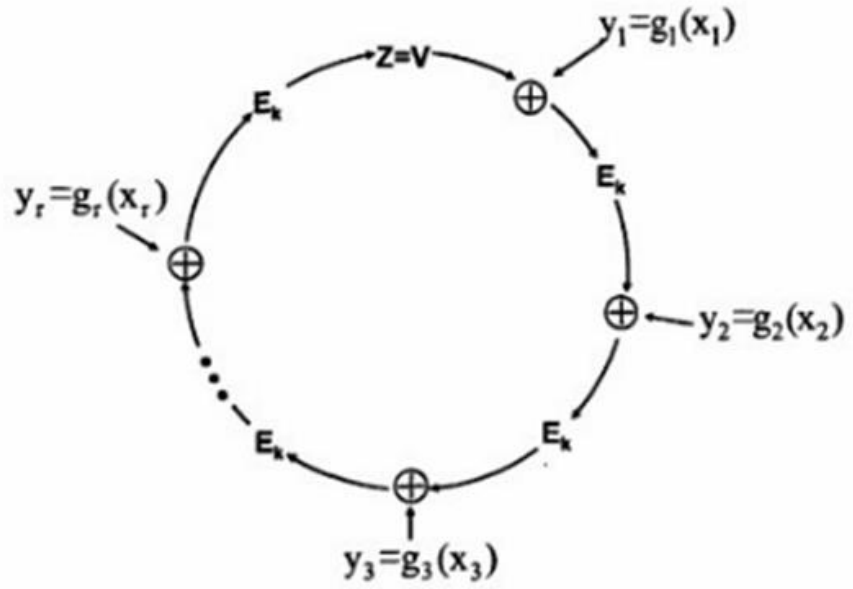
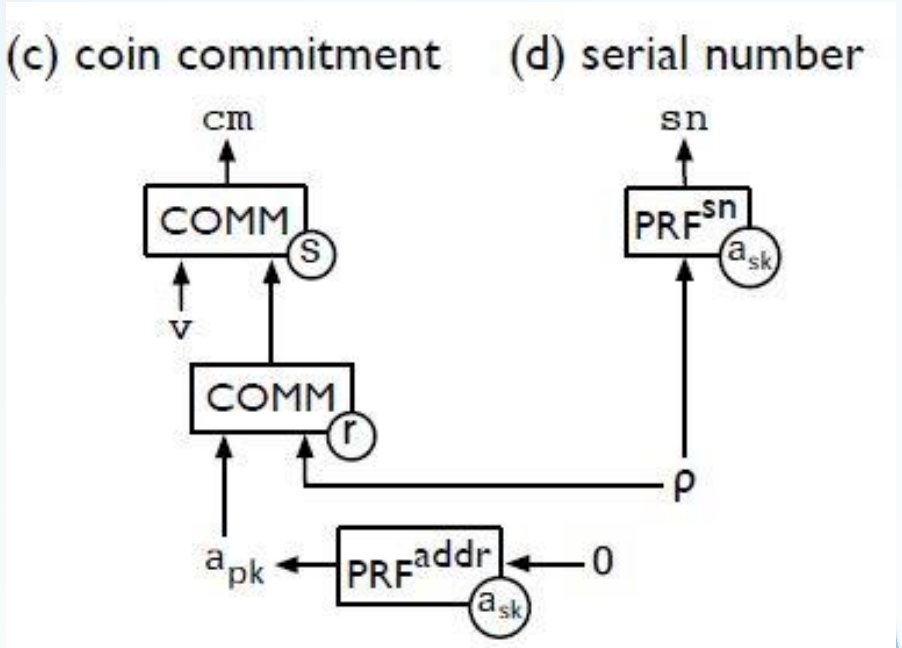


图1.1 Rivest 等提出的环签名算法示意图

Fig.1.1 The Ring Signature Scheme Proposed by Rivest et al.

Zerocash（ZK-SNARKs）

--铸币交易（Mint）



--转账交易Pour

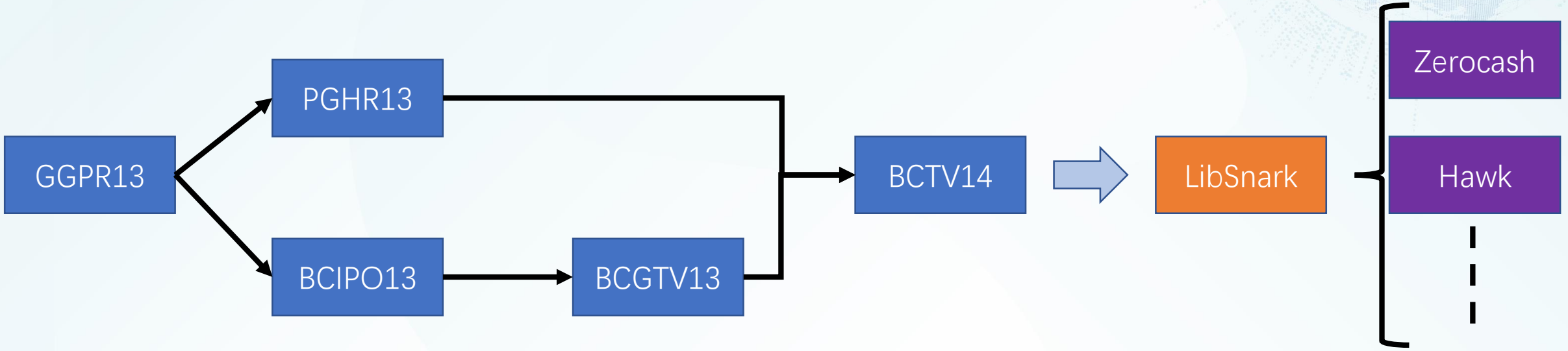
$$\mathbf{c} = (a_{pk}, v, r, s, \rho, cm, sn)$$

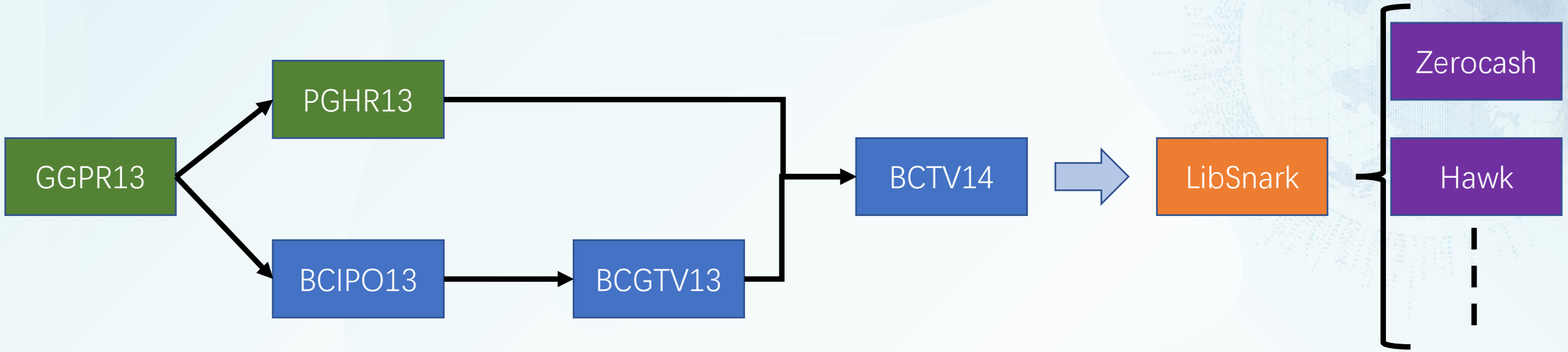
$$\mathbf{c_1} = (b_{pk}, y, \rho_1, r_1, s_1, cm_1)$$

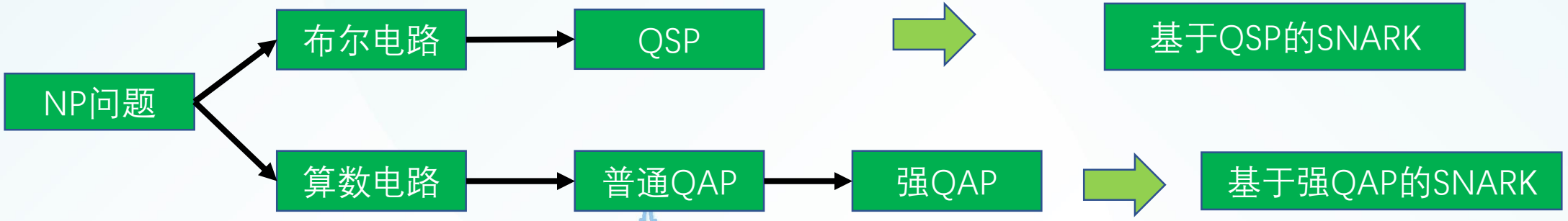
$$\mathbf{c_2} = (a_{pk}, v - y, \rho_2, r_2, s_2, cm_2)$$ （找零）

将如下交易信息发送到公网上：$TX_{pour} = (sn, cm_1, cm_2, \pi)$.

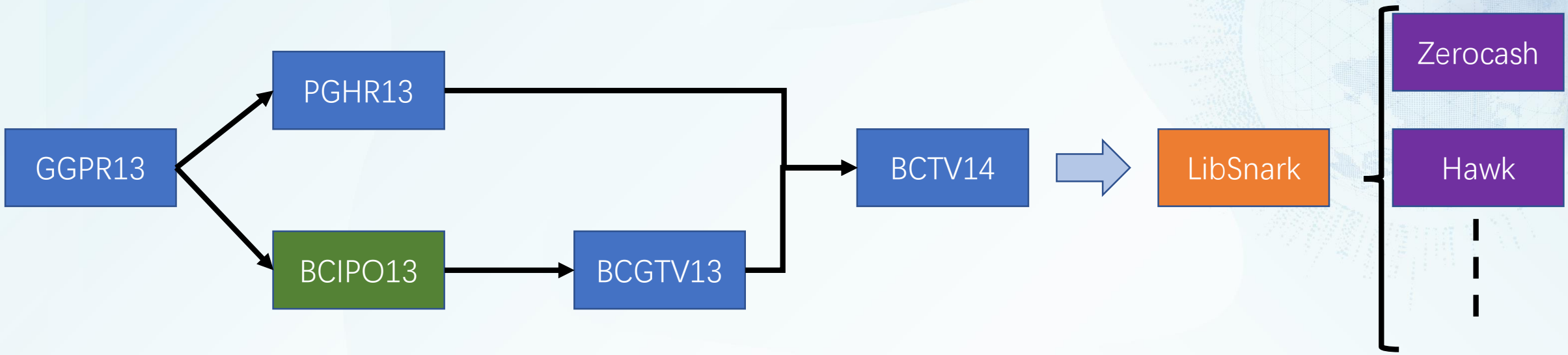
SNARK


GGPR13
PGHR13
BCIPO13
BCGTV13
BCTV14
LibSnark
Zerocash
Hawk



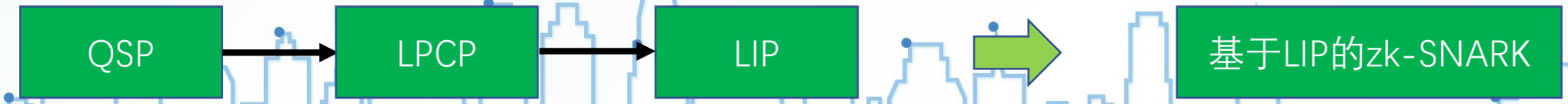


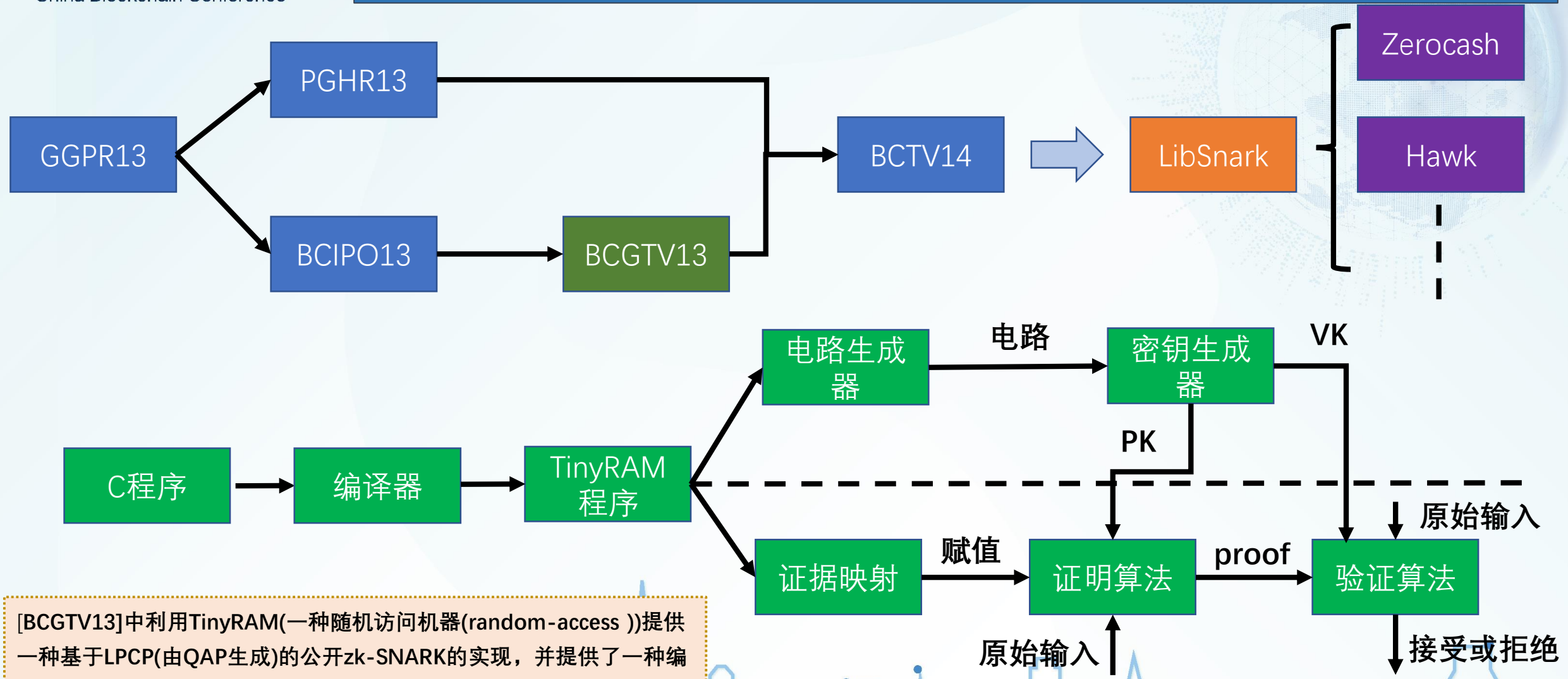
[PGHR13]在[GGPR13]的基础上提出了基于普通QAP而非强QAP(其次数将近是普通QAP的三倍)下的接近实用的SNARK方案。并提供一种编译器可以将C程序转换成相对应的算术电路。



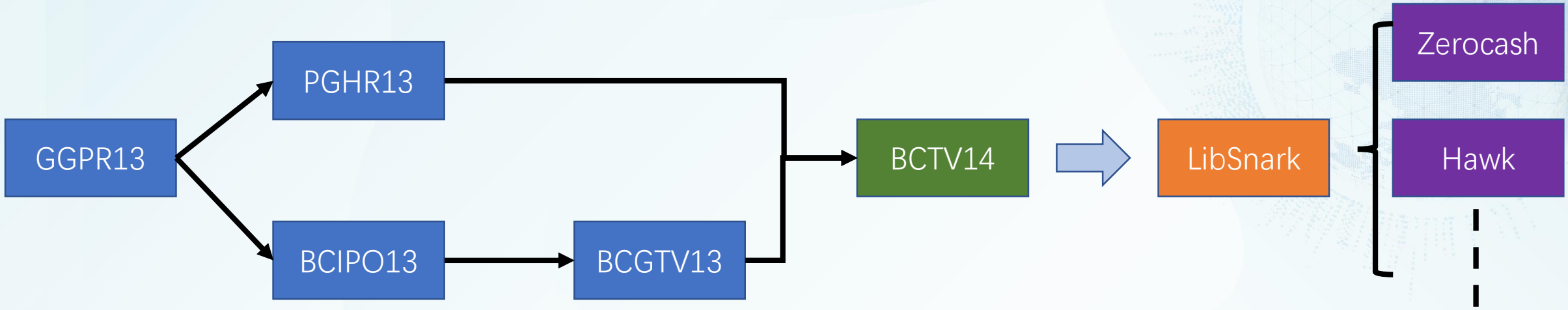
- **BCIPO13**

[BCIPO13]中提出了一种从LPCP(linear Probabilistically checkable Proof)转换成线性交互证明(linear interactive proof，LIP)的技术，并在LIP上设计zk-SNARK方案。





[BCGTV13]中利用TinyRAM(一种随机访问机器(random-access))提供一种基于LPCP(由QAP生成)的公开zk-SNARK的实现，并提供了一种编译器可以将C程序转换成相对应的TinyRAM程序。

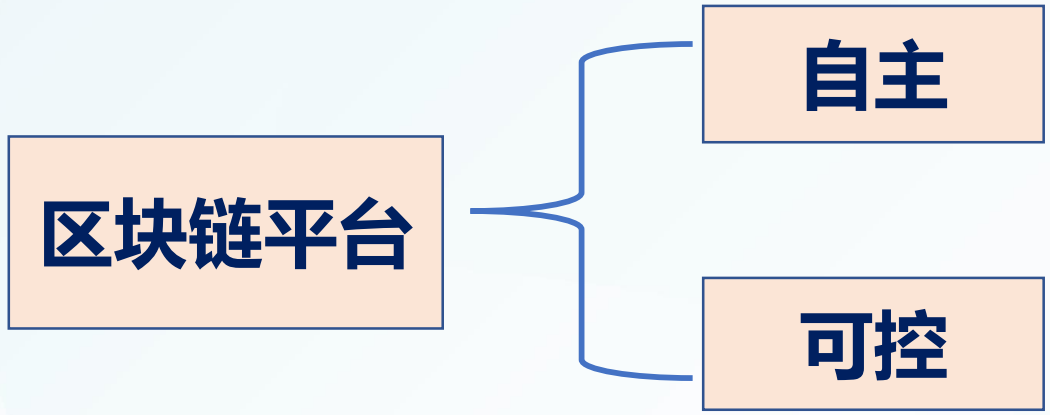


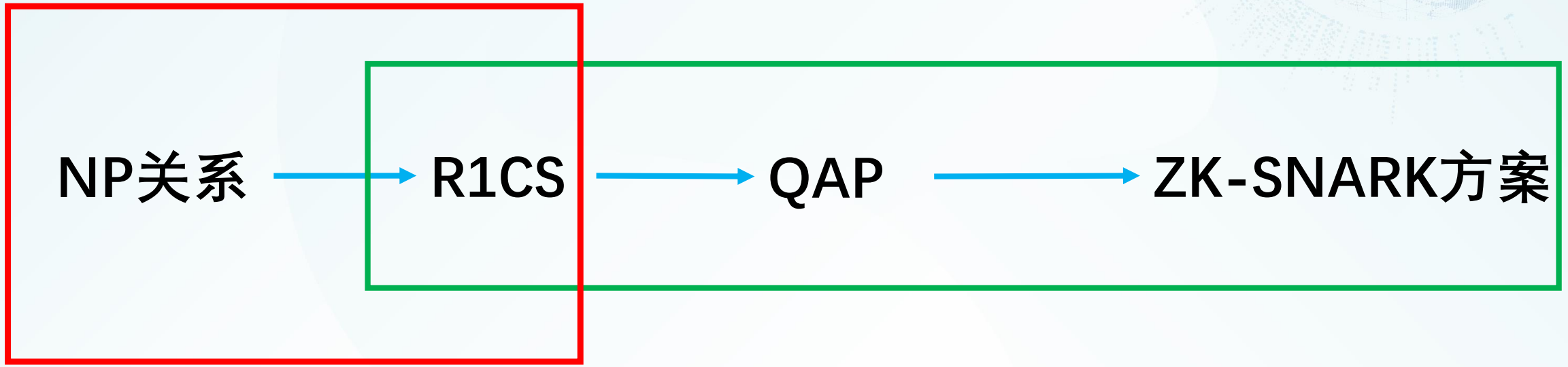
[BCTV14]中实现了一种zk-SNARK系统。此系统对[PGHR13]中方案进行了优化，改进了证明与验证的时间。

- 在[BCGTV13]的TinyRAM的基础上提出了适用于冯诺依曼体系结构的vnTinyRAM，并提供了可将C程序编译成vnTinyRAM机器语言的编译器。
- 他们所设计的电路生成器相比与之前的实现([BCGTV13]，[PGHR13])的优势：
  - 电路生成是通用(Universal)的，即不依赖于程序；
  - 可以很高效地处理任意较大型的程序。

China Blockchain Conference

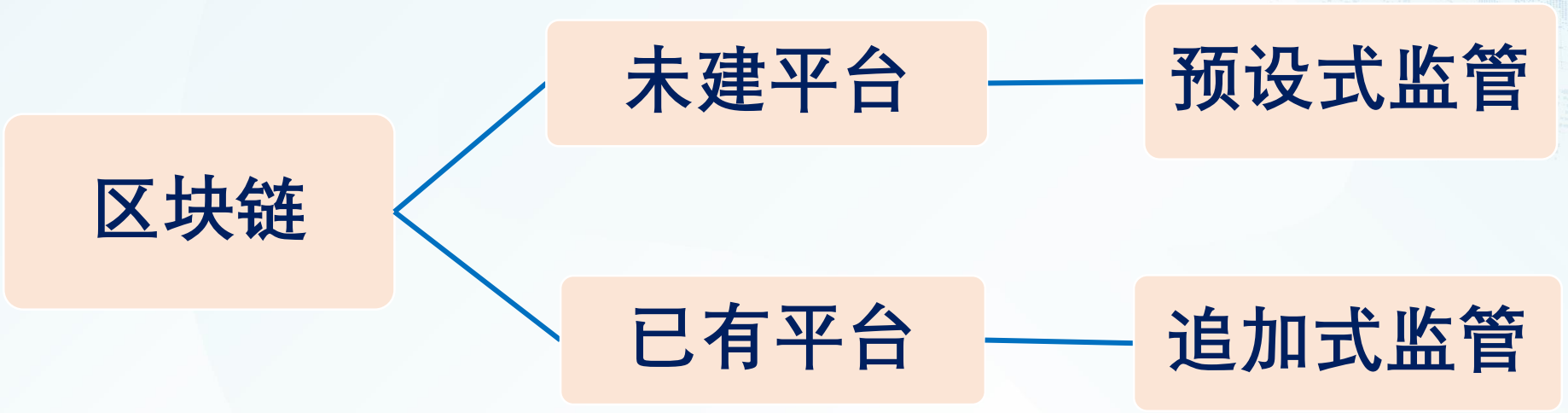
目录

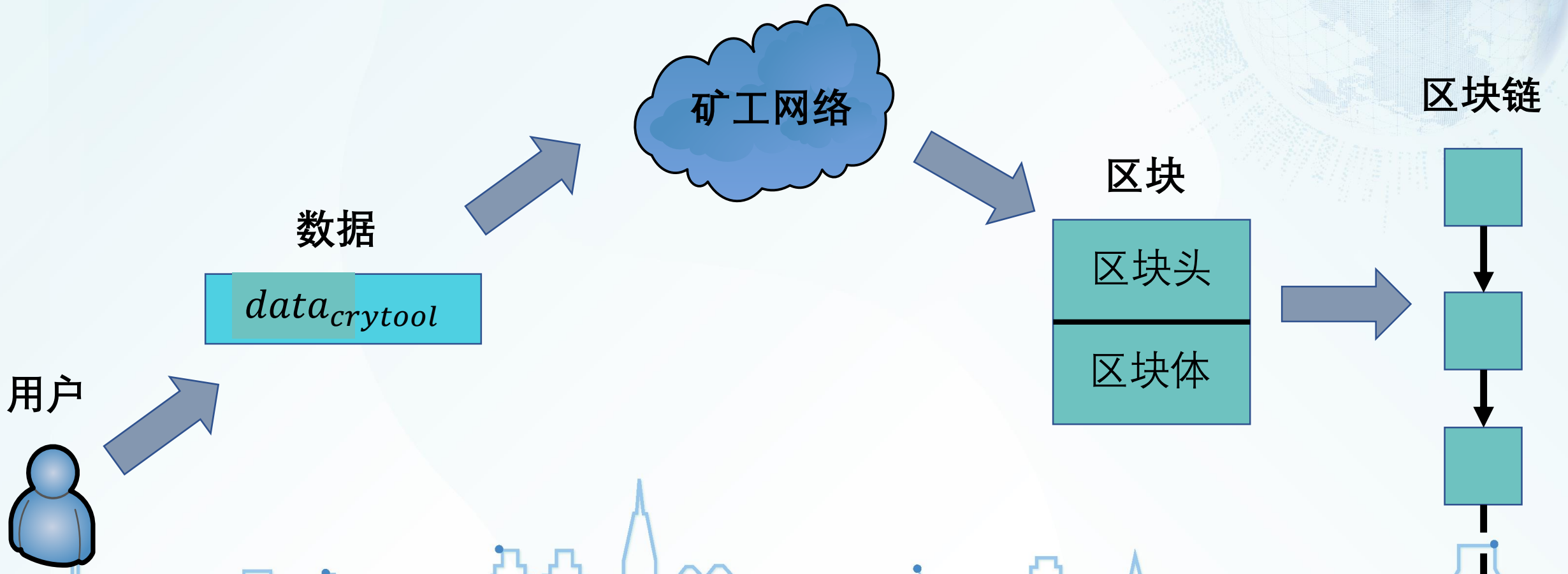

区块链平台
自主
可控

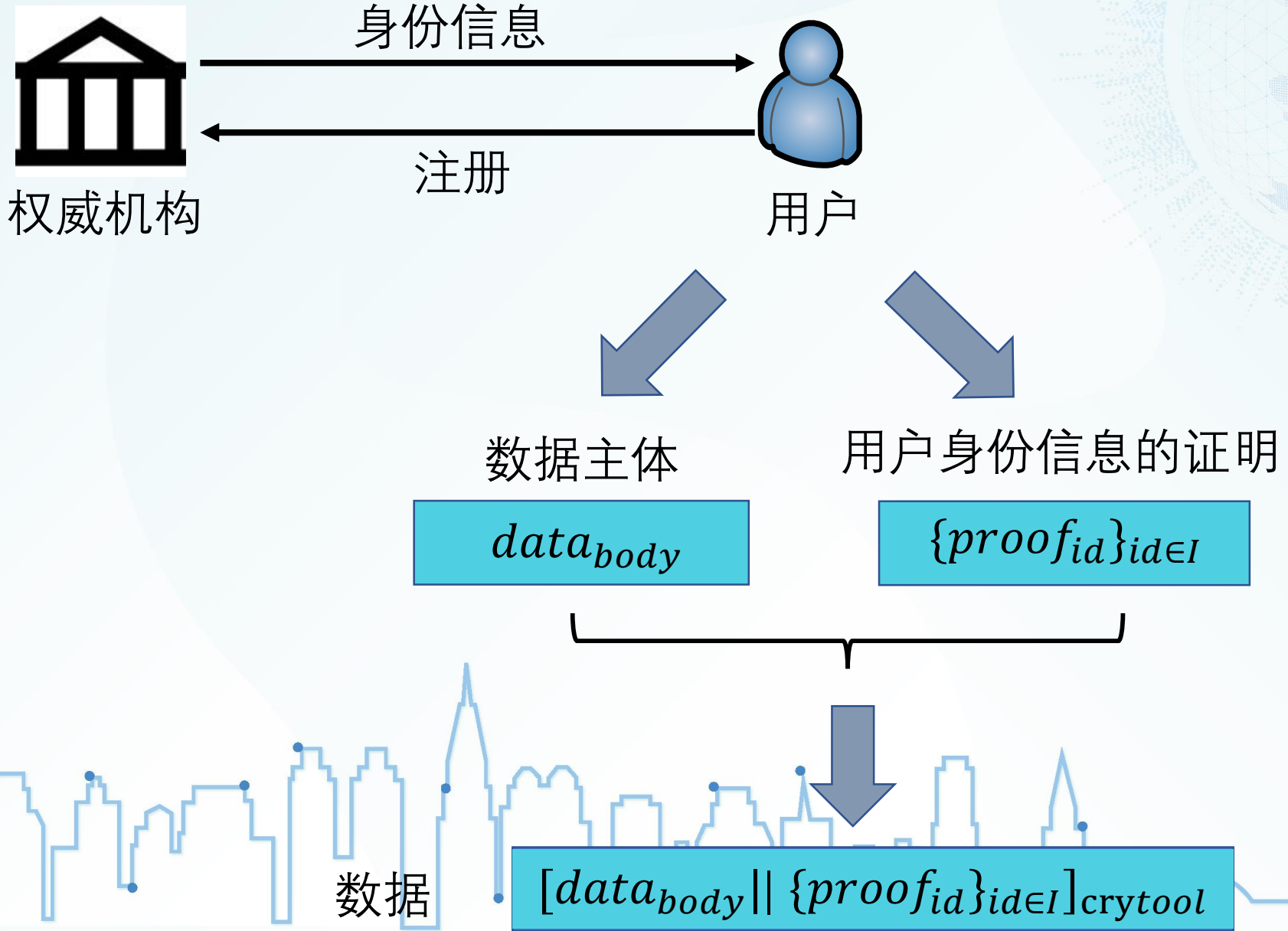

NP关系
R1CS
QAP
ZK-SNARK方案

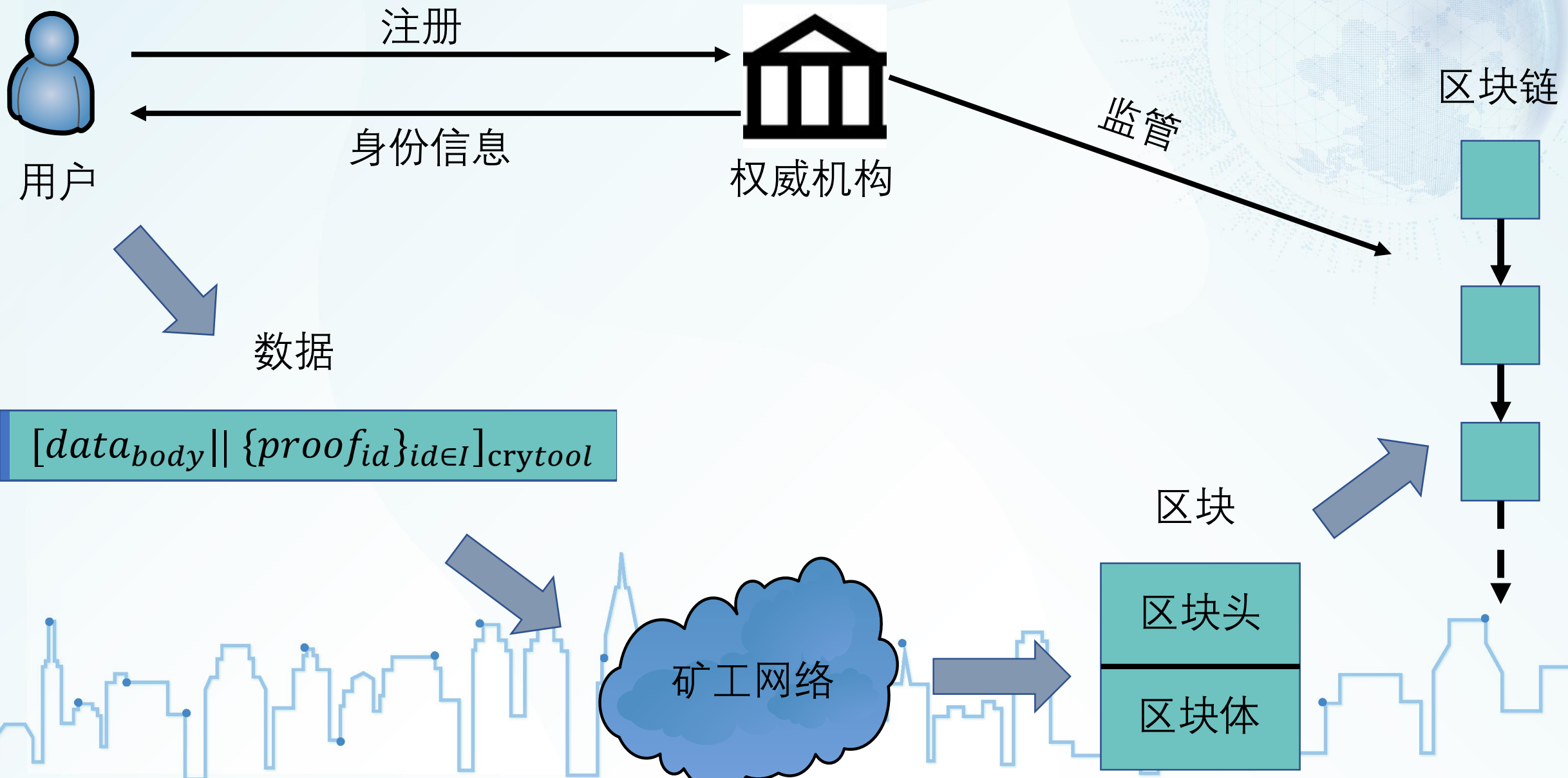
libsnark中提供了4条椭圆曲线

- Edwards曲线
- Barreto-Naehrig曲线
- MNT4曲线
- MNT6曲线


区块链
未建平台
预设式监管
已有平台
追加式监管


矿工网络
区块链
区块
数据
区块头
$data_{crytool}$
区块体
用户


身份信息
注册
权威机构
用户
数据主体
用户身份信息的证明
$data_{body}$
$\{proof_{id}\}_{id \in I}$
数据
$[data_{body} || \{proof_{id}\}_{id \in I}]_{crytool}$


注册
身份信息
用户
权威机构
监管
区块链
数据
$[data_{body} || \{proof_{id}\}_{id \in I}]_{crytool}$
区块
矿工网络
区块头
区块体

感谢倾听！ 敬请指正！