

区块链全景图

Tim (i@timqi.com 20180301)

本次分享

➤ 技术篇

- 区块链、共识协议

- 智能合约

➤ 产业篇

- 矿机、矿场、矿池

- 交易所、OTC、（硬）钱包

- 币的发行、ICO、硬分叉

➤ 玄学篇

技术篇

“

财产转移是经多数人见证达成的共识

技术篇 · 状态转换

1. 交易的每个输入：
 - 如果引用的UTXO (unspent transaction outputs) 不存在于现在的状态中 (S)，返回错误提示
 - 如果签名与UTXO所有者的签名不一致，返回错误提示
2. 如果所有的UTXO输入面值总额小于所有的UTXO输出面值总额，返回错误提示
3. 返回新状态S',新状态S中移除了所有的输入UTXO，增加了所有的输出UTXO。

技术篇 · 状态转换

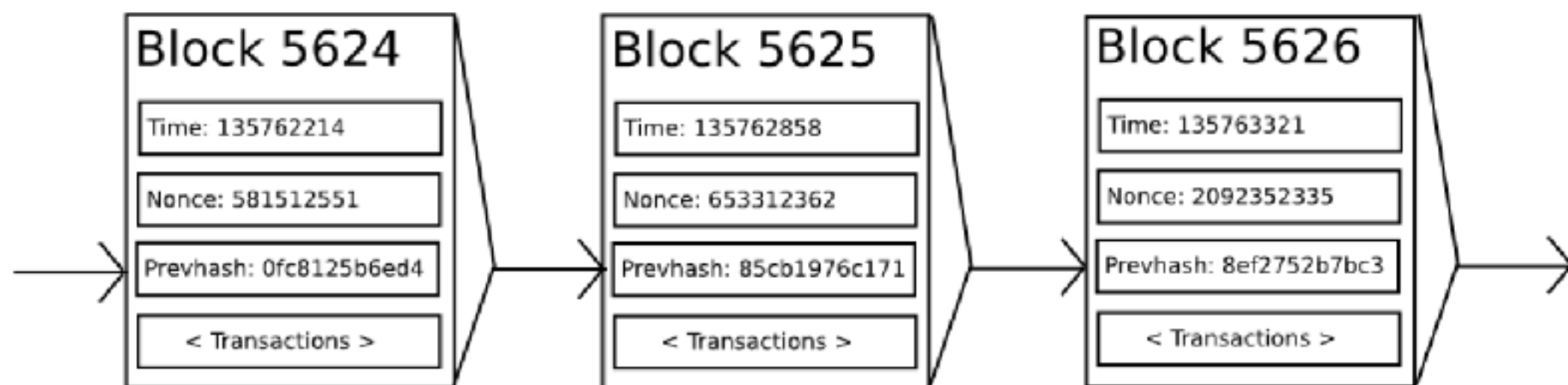
APPLY(S, TX) > S' or ERROR

APPLY({ Alice: \$50, Bob: \$50 }, "send \$20 from Alice to Bob") = { Alice: \$30, Bob: \$70 }

APPLY({ Alice: \$50, Bob: \$50 }, "send \$70 from Alice to Bob") = ERROR

技术篇 · 区块链

.....

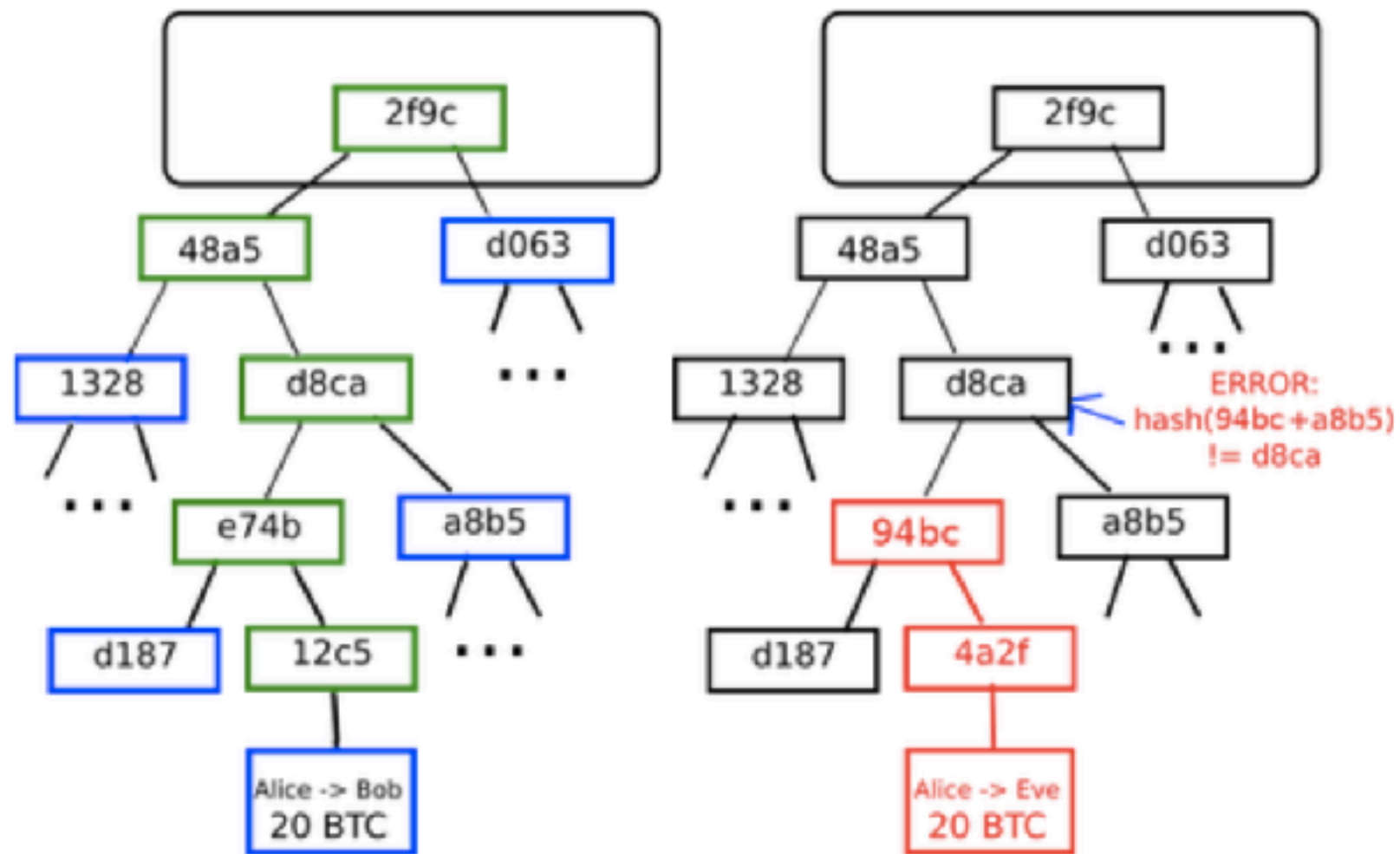


技术篇·区块验证

1. 检查区块引用的上一个区块是否存在且有效。
2. 检查区块的时间戳是否晚于以前的区块的时间戳，而且早于未来2小时。
3. 检查区块的工作量证明是否有效。
4. 将上一个区块的最终状态赋于S[0]。
5. 假设TX是区块的交易列表，包含n笔交易。对于属于0.....n-1的所有i,进行状态转换 $S[i+1] = \text{APPLY}(S[i], \text{TX}[i])$ 。如果任何一笔交易i在状态转换中出错，退出程序，返回错误。
6. 返回正确，状态S[n]是这一区块的最终状态。

技术篇 • MERKLE TREES

.....



技术篇 · 共识算法

- PoW (Proof of Work)
- PoS (Proof of Stake)
- DPoS (Delegated Proof of Stake)

技术篇 • PROOF OF WORK

$$H(B) \leq m$$

技术篇 • PROOF OF STAKE

$$H(H(B_{prev}), A, t) \leq balance(A)m$$

技术篇 • DELEGATED PROOF OF STAKE

通过不同的策略，不定时的选中一小群节点，这一小群节点做**新区块的创建，验证，签名和相互监督**，这样就大幅度的减少了区块创建和确认所需要消耗的时间和算力成本

技术篇·其他规则

- 挖矿收益，每四年减半
- BTC 总量2100万个
- m 随着挖矿算 调节的 $H(ts + n) < m$

技术篇・潜在攻击方法

.....

攻击方法	PoW	PoS	DPoS
短距离攻击（如贿赂攻击）	－	＋	－
长距离攻击	－	＋	＋
币龄累计攻击	－	＋	＋
预计算攻击	－	＋	－
DDos	－	可能	－
女巫攻击（Sybil Attack）	＋	＋	＋

“

共识算法产生信任，造成生产关系改变

“

密码学保证了记账权博弈的均衡

技术篇·基于比特币的应用

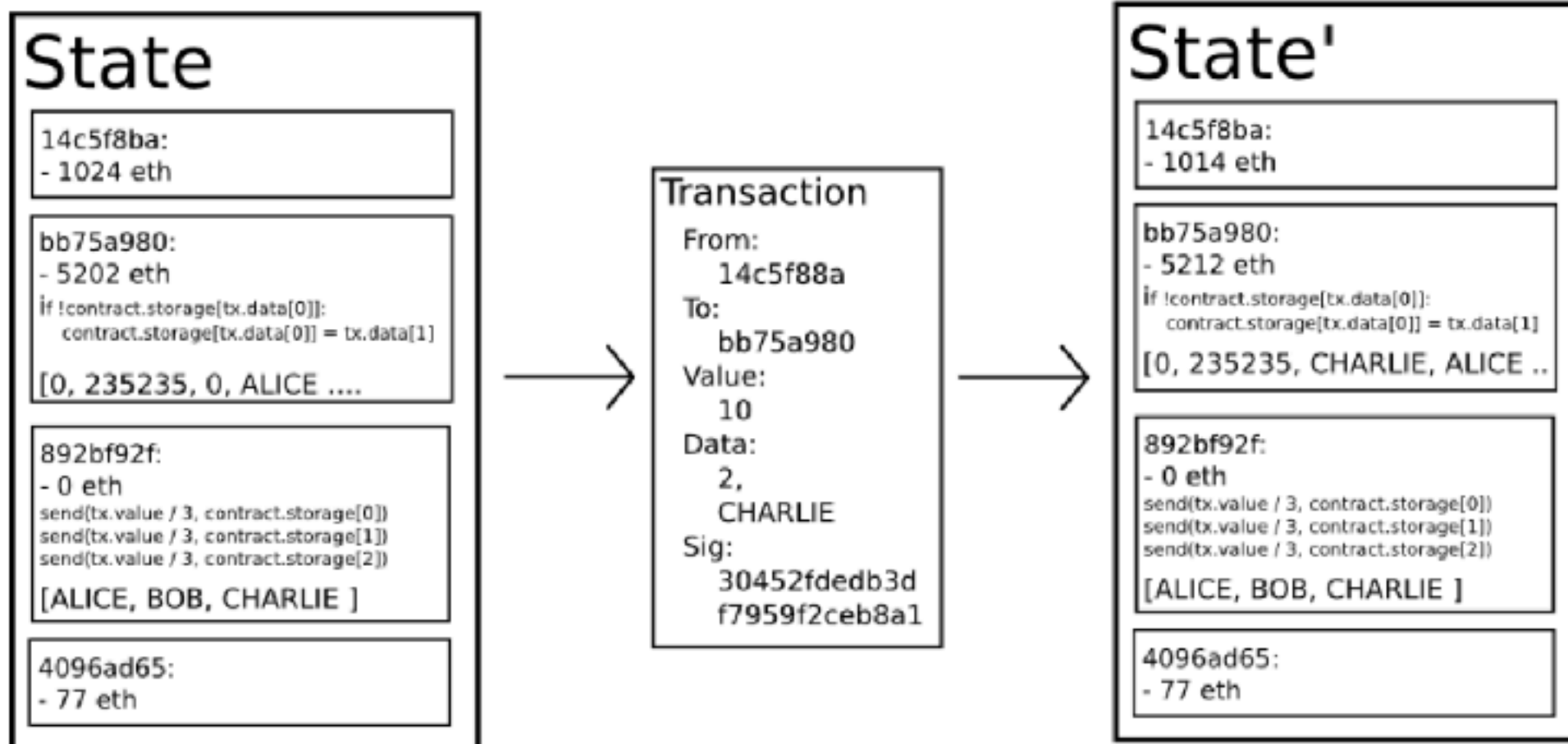
- 域名币（**namecoin**） - 只有第一个注册者可以成功注册，第二个不能再次注册同一个账户。这一问题就可以利用比特币的共识协议。域名币是利用区块链实现名称注册系统的最早的、最成功的系统。
- 彩色币（**Colored coins**） - 彩色币的目的是为人们在比特币区块链上创建自己的数字货币，人们可以通过为某一特别的比特币UTXO指定颜色，发行新的货币。发送这些UTXO就像发送普通的比特币一样，通过回溯全部的区块链判断收到的UTXO颜色。

技术篇·比特币脚本限制

- 缺少图灵完备性 – 最主要的缺失是循环语句
- **Value-blindness** - UTXO脚本不能为账户的取款额度提供精细的控制
- 缺少状态 – UTXO只能是已花费或者未花费状态
- **Blockchain-blindness** - UTXO看不到区块链的数据

技术篇 · 以太坊状态转换

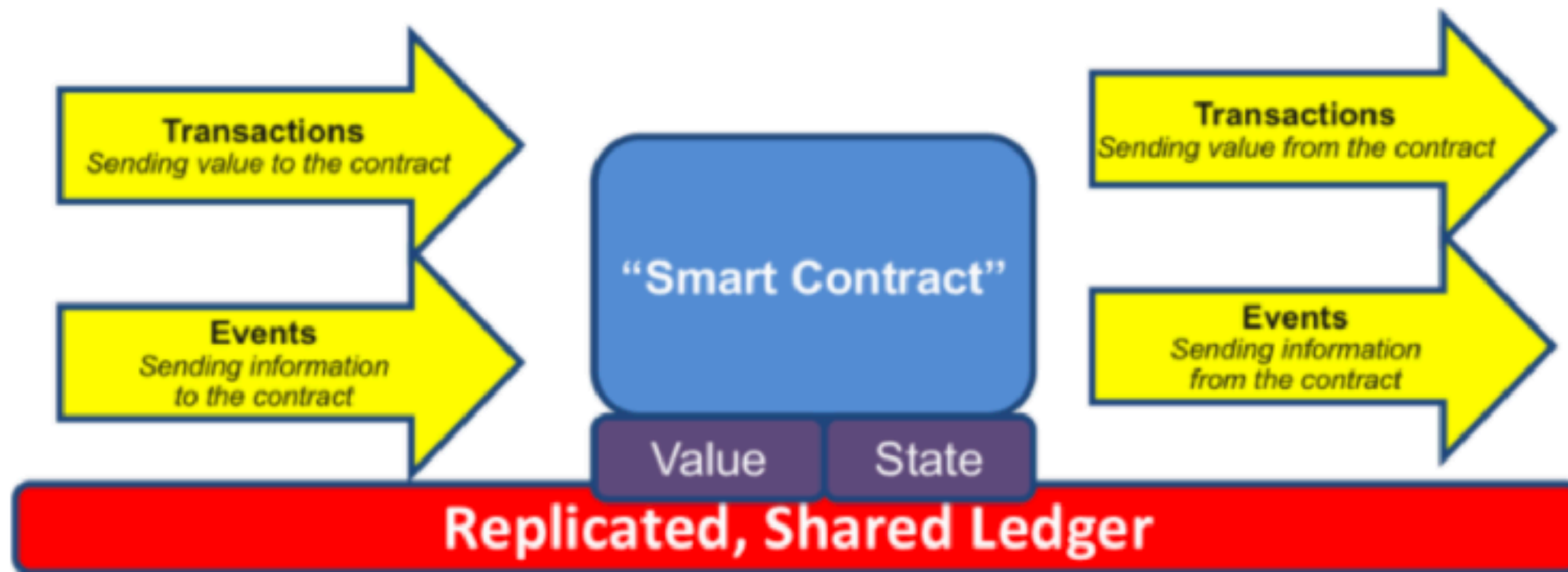
.....



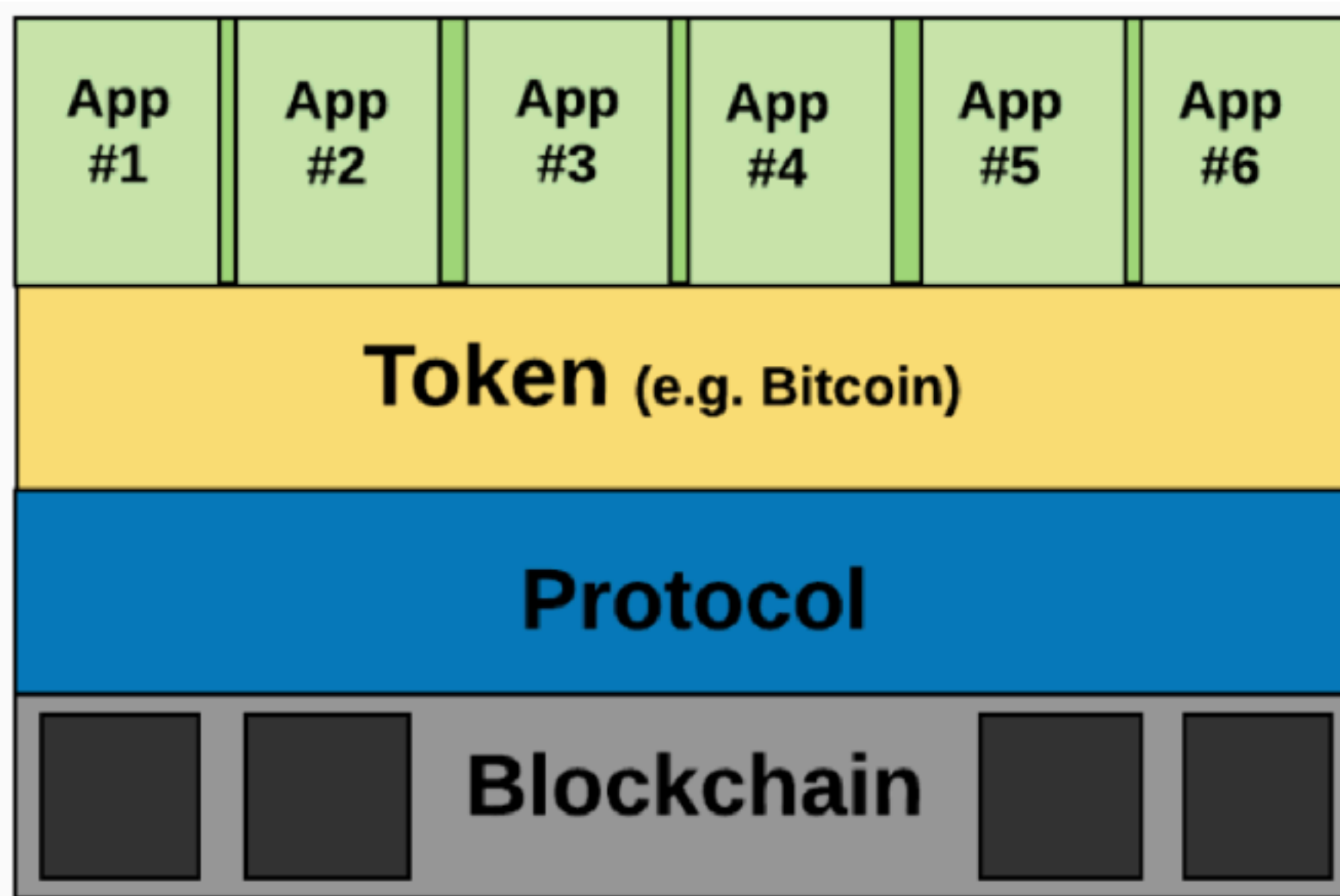
技术篇·以太坊状态转换函数

1. 检查交易的格式是否正确（即有正确数值）、签名是否有效和随机数是否与发送者账户的随机数匹配。如否，返回错误。
2. 计算交易费用: $\text{fee} = \text{STARTGAS} * \text{GASPRICE}$ ，并从签名中确定发送者的地址。从发送者的账户中减去交易费用和增加发送者的随机数。如果账户余额不足，返回错误。
3. 设定初值 $\text{GAS} = \text{STARTGAS}$ ，并根据交易中的字节数减去一定量的瓦斯值。
4. 从发送者的账户转移价值到接收者账户。如果接收账户还不存在，创建此账户。如果接收账户是一个合约，运行合约的代码，直到代码运行结束或者瓦斯用完。
5. 如果因为发送者账户没有足够的钱或者代码执行耗尽瓦斯导致价值转移失败，恢复原来的状态，但是还需要支付交易费用，交易费用加至矿工账户。
6. 否则，将所有剩余的瓦斯归还给发送者，消耗掉的瓦斯作为交易费用发送给矿工。例如，假设合约的代码如下：

技术篇·智能合约



技术篇 · 架构

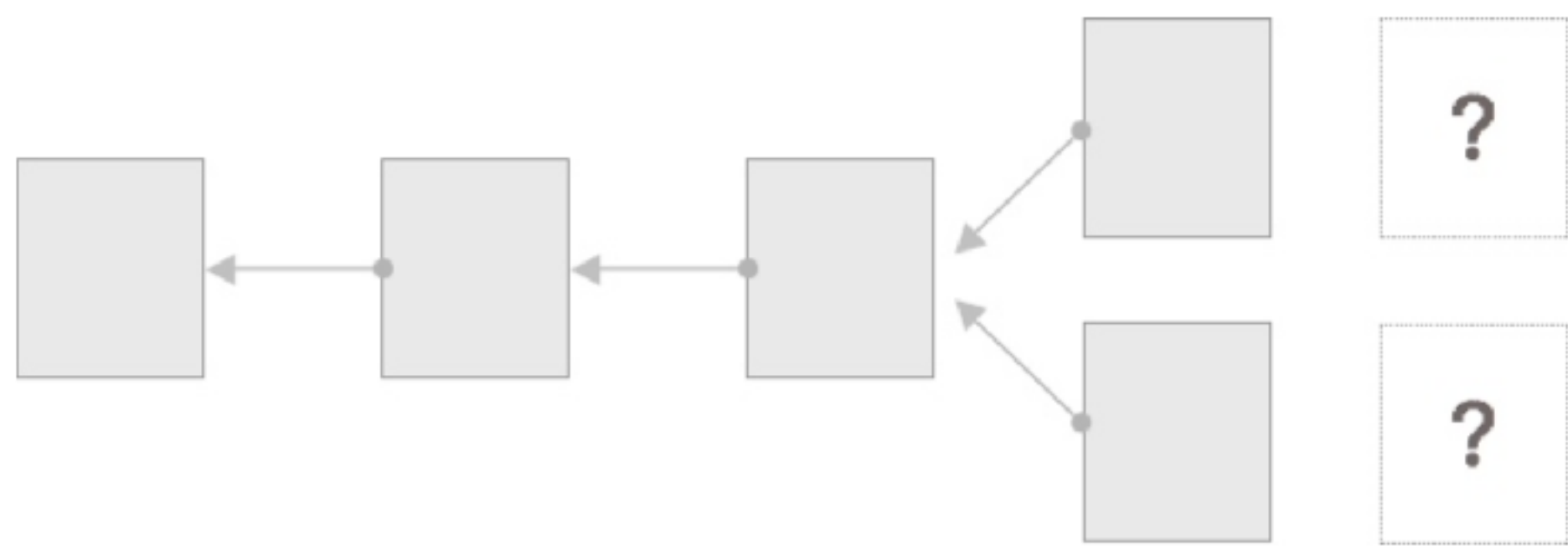


技术篇 • ERC20

- Token 名称
- Token 发总数
- 符号，如 BNB
- 转账
- 提现
- 其他

技术篇 · 分叉

.....



技术篇·升级方案

1. 提高区块大小，比如第一次硬分叉后，比特现金把区块大小提升到了8M区块
2. 提升出块效率，并同比降低出块奖励，以太坊的出块速度就明显比比特币要快的多
3. 区块分片化存储的方案，现在比特币这样的区块链虽然是去中心化分布式存储，但每个全节点存储的是记录全集
4. 闪电网络是指将小额的，频繁交易，先通过一些分支节点进行储存和计算，并在一定时间内整合归并到主链

产业篇

产业篇·矿机

.....



产业篇·矿机

.....

蚂蚁矿机S9规格参数

- 1.额定算力: 13.5 TH/s的 $\pm 5\%$
- 2.墙上功耗: 1350瓦 $\pm 12\%$ (普通版 APW3++ 电源, AC/DC 93%的效率, 25℃环境温度)
- 3.电源效率: 0.1J/GH $\pm 12\%$ (墙上, AC/DC 93%的效率, 25° C的环境温度)
- 4.额定电压: 11.6~13.0V
- 5.芯片数量: 189片 BM1387
- 6.外箱尺寸: 445毫米(L) * 215毫米(W) * 255毫米(H)
- 7.冷却: 2×12038风扇
- 8.工作温度: 0℃至40℃
- 9.工作湿度: 5%RH~95%RH, 非凝露
- 10.网络连接: 以太网




















产业篇·矿场

.....



产业篇·矿池

					24小时变化	3天幸运值
1	 BTC.com	<div><div></div></div>	5690.00	PH/s	0.32%	116.28%
2	 AntPool	<div><div></div></div>	3667.27	PH/s	-0.41%	72.42%
3	 ViaBTC	<div><div></div></div>	2752.02	PH/s	0.12%	82.89%
4	 SlushPool	<div><div></div></div>	2223.04	PH/s		-
5	 F2Pool	<div><div></div></div>	1401.48	PH/s		-
6	 BTCC	<div><div></div></div>	958.95	PH/s	0.08%	114.51%
7	 BTC.TOP	<div><div></div></div>	535.00	PH/s	12.39%	211.77%
8	 Bitcoin.com	<div><div></div></div>	534.03	PH/s	80.71%	83.77%
9	 BitClub	<div><div></div></div>	469.39	PH/s	-0.49%	85.09%
10	 58COIN	<div><div></div></div>	386.62	PH/s		-
11	 CanoePool	<div><div></div></div>	338.29	PH/s		-
12	 BitFury	<div><div></div></div>	289.96	PH/s		-

产业篇·挖矿

比特币现在年产出是多少，每10分钟一个区块，每个区块12.5个比特币奖励，算下来一年有65万比特币产出，以太坊新版本降低了奖励，目前差不多每12秒挖出一个块，每块差不多3.3个以太币奖励，所以每年差不多有800多万的以太币产出，过去是1100万左右

产业篇·交易所



产业篇·去中心化交易所

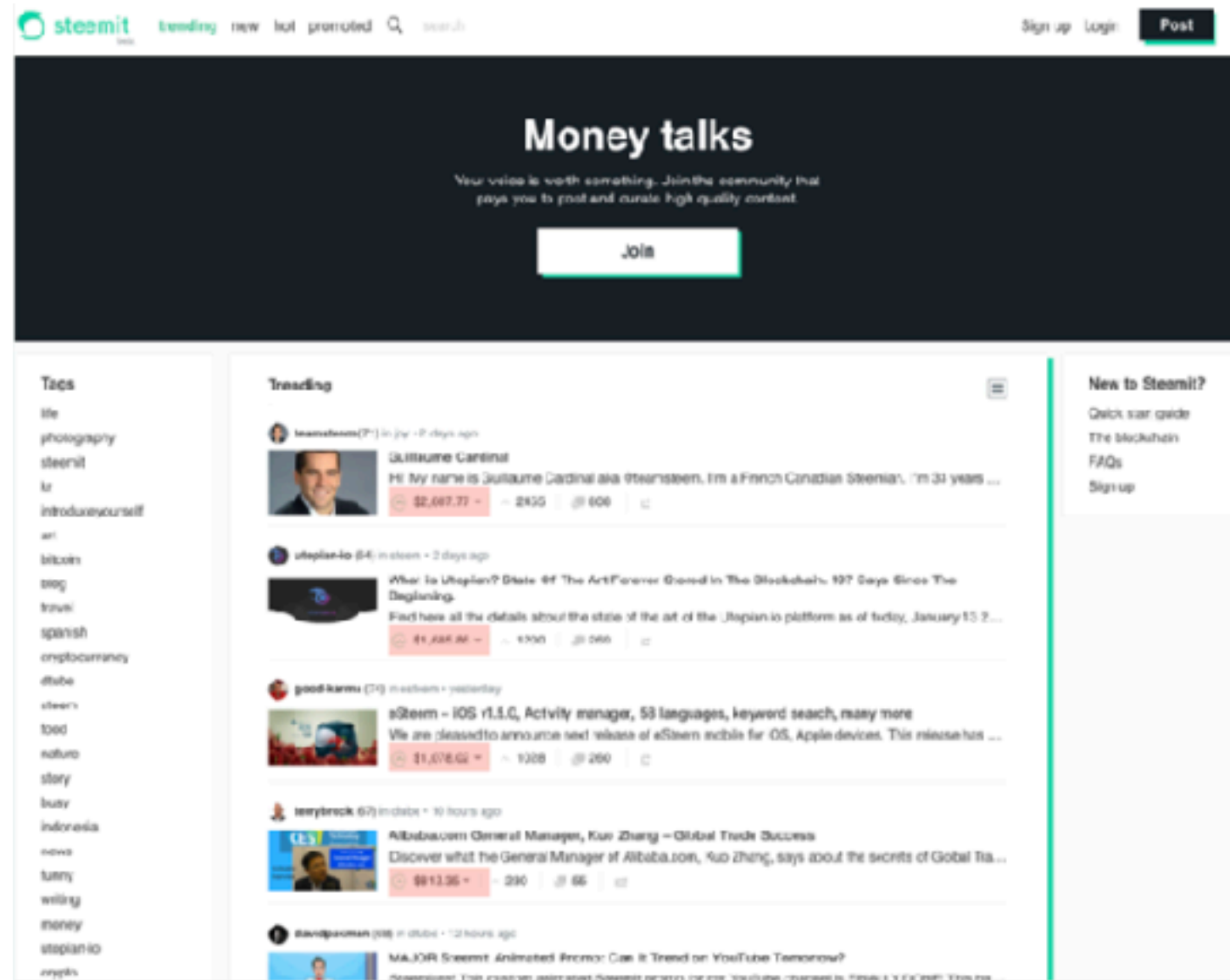


RADAR RELAY

产业篇·交易所

虚拟币1198种，代币687种，交易平台254个，24小时成交量1.3千亿人民币。如果按照千二手续费计算每天手续费大概3~5亿，一年差不多在**千亿**级别

产业篇·应用举例



产业篇·应用举例

.....



A MASSIVE AMOUNT OF STORAGE SITS UNUSED IN DATA CENTERS AND HARD DRIVES AROUND THE WORLD.



EARN FILECOIN FOR HOSTING FILES

Put your unused storage to work by becoming a Filecoin miner. Use the [Filecoin website](#) to learn more about how to get started.



EXCHANGE FILECOIN FOR USD, BTC, ETH AND MORE

The Filecoin currency will be traded on a number of exchanges and supported by a number of wallets. [Check out the list of supported wallets and exchanges.](#)



RELIABLY STORE FILES AT HYPERCOMPETITIVE PRICES

Clients can tune their storage strategy to suit their needs, creating a custom [Filecoin storage plan](#) that meets their requirements.

产业篇·应用举例

.....



The screenshot shows the RippleNet website. At the top is a navigation bar with the Ripple logo, a search icon, and links for Solutions, Use Cases, ERP, Resource, About, and a Contact button. The main header area has a dark blue background with a geometric pattern and the text 'Join RippleNet' and 'The world's only enterprise blockchain solution for global payments'. A 'Watch Video' button is also present. Below this, a section titled 'Today's Payment Rails Don't Cut It' contains a paragraph about the limitations of current payment systems. To the right of the text is a diagram with three interconnected hexagonal nodes, each representing a different pain point: 'SLOW' (3-5 days to settle), 'UNRELIABLE' (high failure rates), and 'UNACCEPTABLE' (people demand a seamless and elegant experience). A fourth node, 'EXTENSIVE' (\$1.5 trillion in annual costs), is also shown. At the bottom of the diagram is a red line. The footer of the page features a light blue background with a geometric pattern and the text 'Meet RippleNet' and 'Ripple connects banks, payment providers, digital asset exchanges and'.

ripple

Solutions - Use Cases - ERP - Resource - About - Contact

Join RippleNet

The world's only enterprise blockchain solution for global payments

Watch Video

Today's Payment Rails Don't Cut It

In a world where three billion people are connected online, cars drive themselves and appliances can communicate, global payments are still stuck in the disco era.

Why? The payment infrastructure was built before the internet with few updates.

SLOW
3-5 days to settle

UNRELIABLE
High failure rates

EXTENSIVE
\$1.5 trillion in annual costs*

UNACCEPTABLE
People demand a seamless and elegant experience

World Trade Organization, Institute of International Finance, Federal Reserve

Meet RippleNet

Ripple connects banks, payment providers, digital asset exchanges and

产业篇·资讯平台

- coinmarketcap.com
- coindesk.com
- aicoi.net.cn
- 金色财经
- 巴比特
- 非小号
- ...

产业篇·传统 VC

.....

ZhenFund

SEQUOIA
红杉中国

matrix
PARTNERS

BANYAN
CAPITAL

M
METROPOLIS VC

INBlockchain

FIBIG
CAPITAL

Nirvana
Capital

Danhua Capital

LINKVC

DFund

NODE CAPITAL
节点资本

FunCity

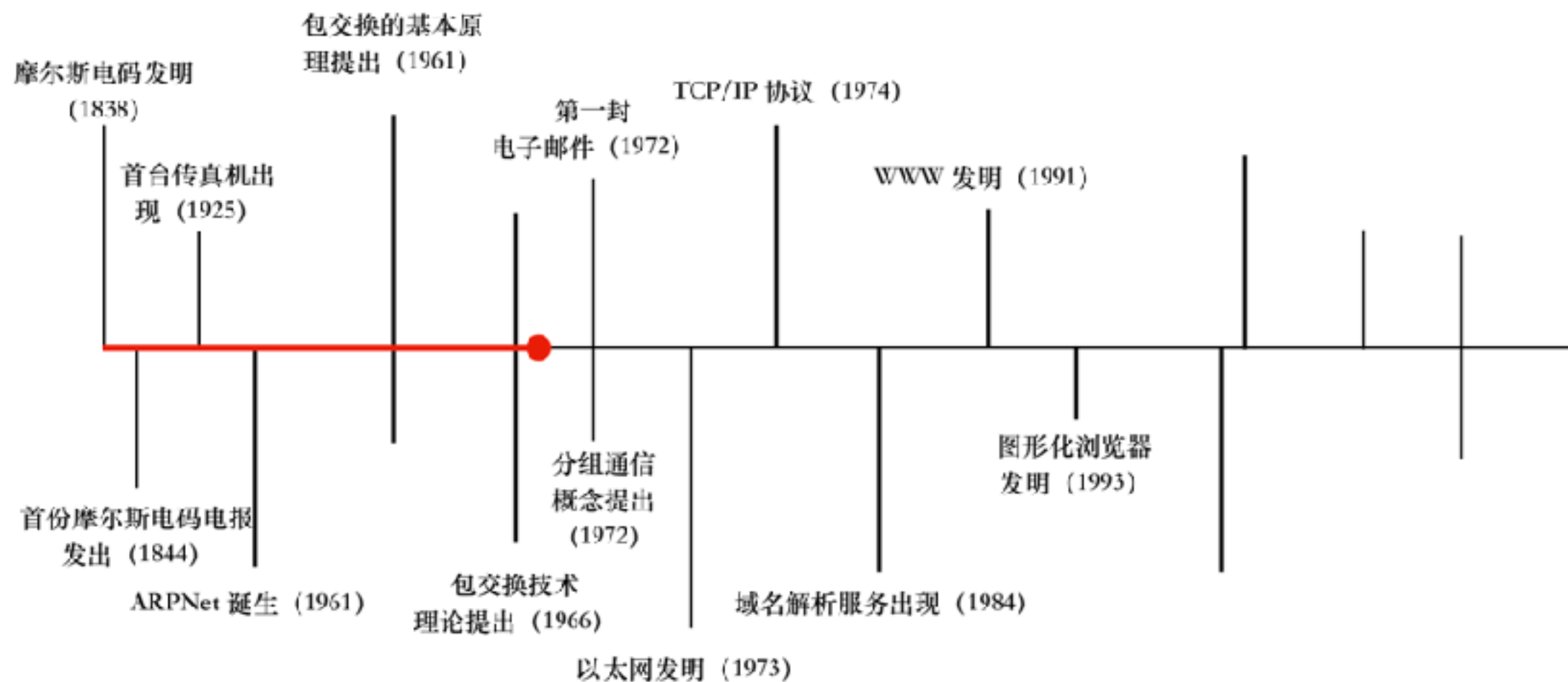
K2VC
陆|峰|张|雷

GENESIS

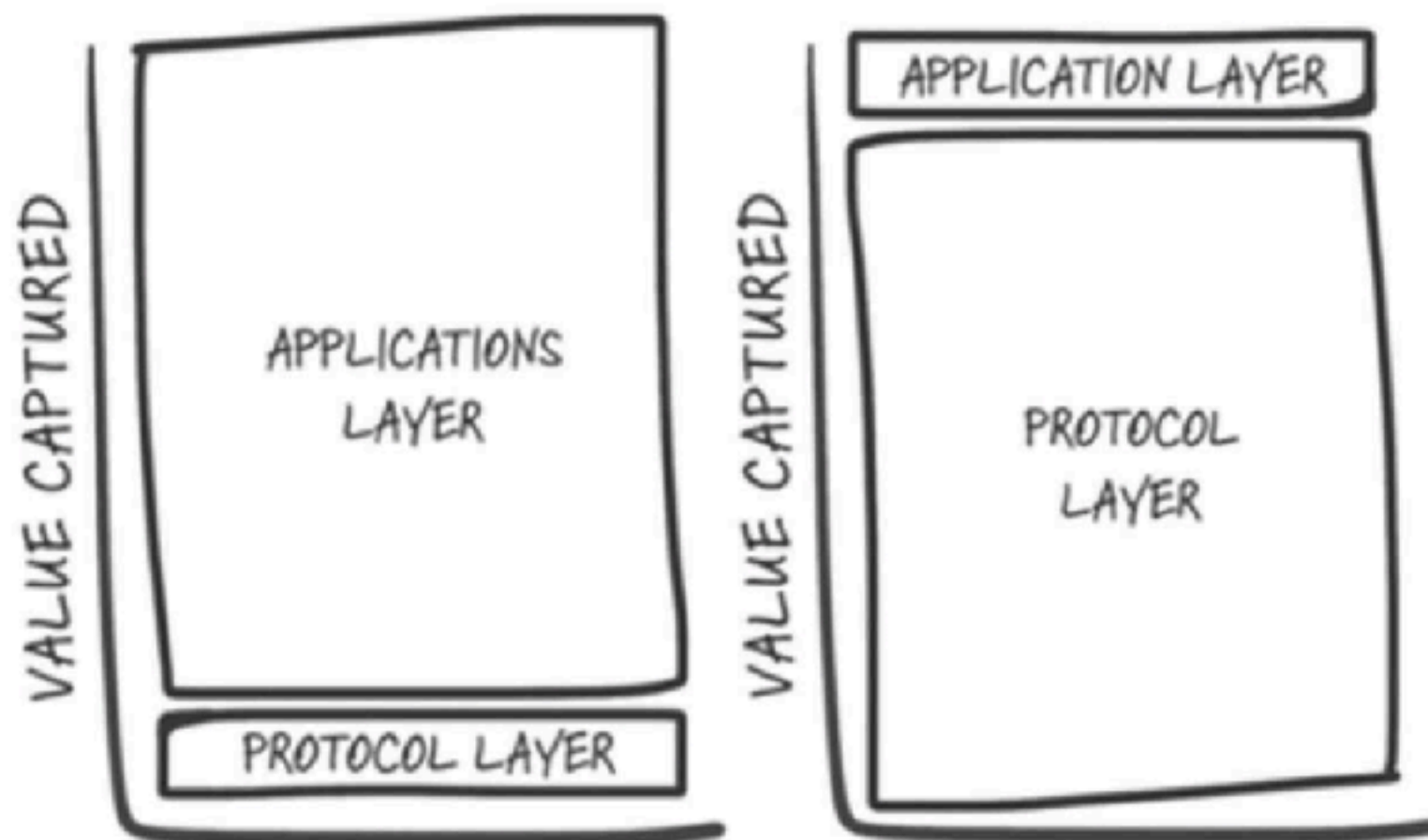
AlphaCoin
Fund

产业篇·当前阶段

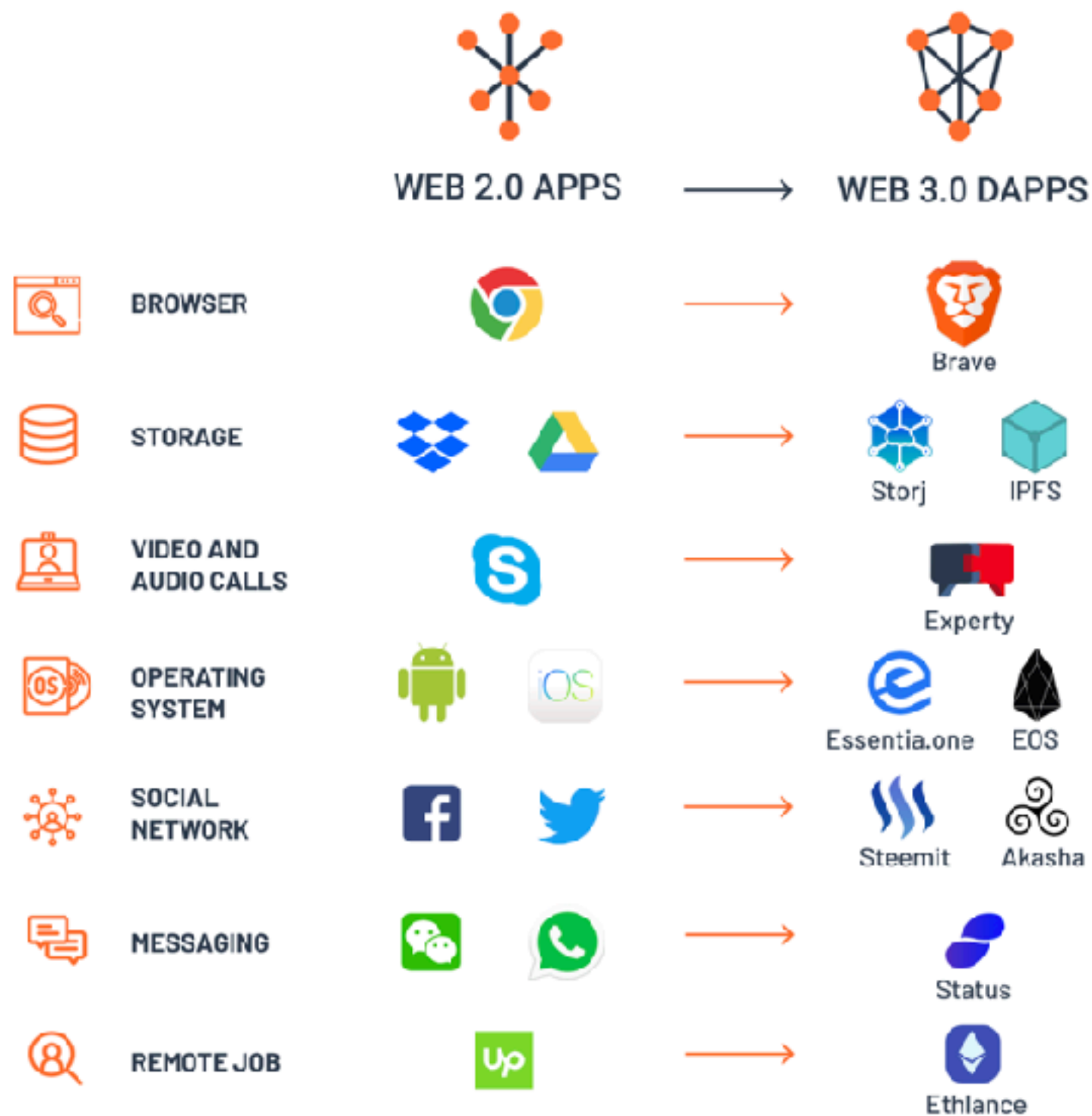
.....



产业篇 • WEB3.0（伪）



产业篇 • (伪)



玄学篇

玄学篇·经济主义

马克思主义

不相信市场经济

凯恩斯主义

摇摆不定

芝加哥学派

有主张，特定时期需要干预

奥地利学派

完全相信市场

“

我相信，世界各国的君主，都是贪婪不公的。他们欺骗臣民，把货币最初所含金属的真实份量，次第削减。

-亚当·斯密 《国富论》

玄学篇·哈耶克






货币的非国家化



作者: [英] 弗里德里希·冯·哈耶克
出版社: 新星出版社
副标题: 对多元货币的理论与实践的分析
原作名: Denationalization of Money
译者: 姚中秋
出版年: 2007-8
页数: 219
定价: 25.00元
装帧: 平装
丛书: 奥地利学派译丛
ISBN: 9787802253162

豆瓣评分

8.9 
416人评价

5星		54.1%
4星		32.5%
3星		11.3%
2星		1.2%
1星		1.0%

玄学篇·津巴布韦

.....



玄学篇·扩张性

以 *AI* 为代表的技术演化减轻了人类作为个体的价值，而区块链是这一变化的**逆过程**，某种程度上讲类似这样的技术变革是必然发生的

玄学篇·信任

区块链降低了组织间、物与物之间的信任成本

玄学篇·资产证券化

区块链将资产证券化，赋予资产流动性
某种意义上流动性就是货币

玄学篇·VIE 结构

.....



内资结构



玄学篇 · CRYPTO 结构



>



>



>



>



>



BNB

币安

OTB

OTCBTC.com

BIG

Big.ONE

JEX

Jex.com

TCH

Cointiger

DEW

DEW.one



OKB

OKEX.com



HT

Huobi.pro

玄学篇·应用

- 共享经济
- 区块链金融
- 物联网
- 数字经济
- 创作激励
- ...

THANKS