公链的演化逻辑和设计

JASON

AMT

区块链对于人类的必要性

人类需要区块链

- 区块链的最重要的核心问题，就是如何解决公开网络上的信任问题。

- 人类为什么需要区块链？因为人类需要更深度和更广范围内达成信任，尤其在数字化时代。
  （工具的演化：易货 贝壳/羽毛/兽皮 金属 纸币 数字货币）

I. 更深度：其它信任源的被信任度受限于人类本身，比如银行，政府，主观/人造产物等用作锚定时，其信任深度不如客观世界存在

II. 更广范围：更广群体间的需求。家人之间不需要，部落间不需要（雅浦岛 石币；邓巴数）

追根溯源：为什么需要更深和更广范围的信任，因为人类要更好地协作。

为什么人类要协作，因为人类要发展

为什么要发展，因为人类追求更长的快乐时间和更短的痛苦时间。

区块链有用，但不是唯一

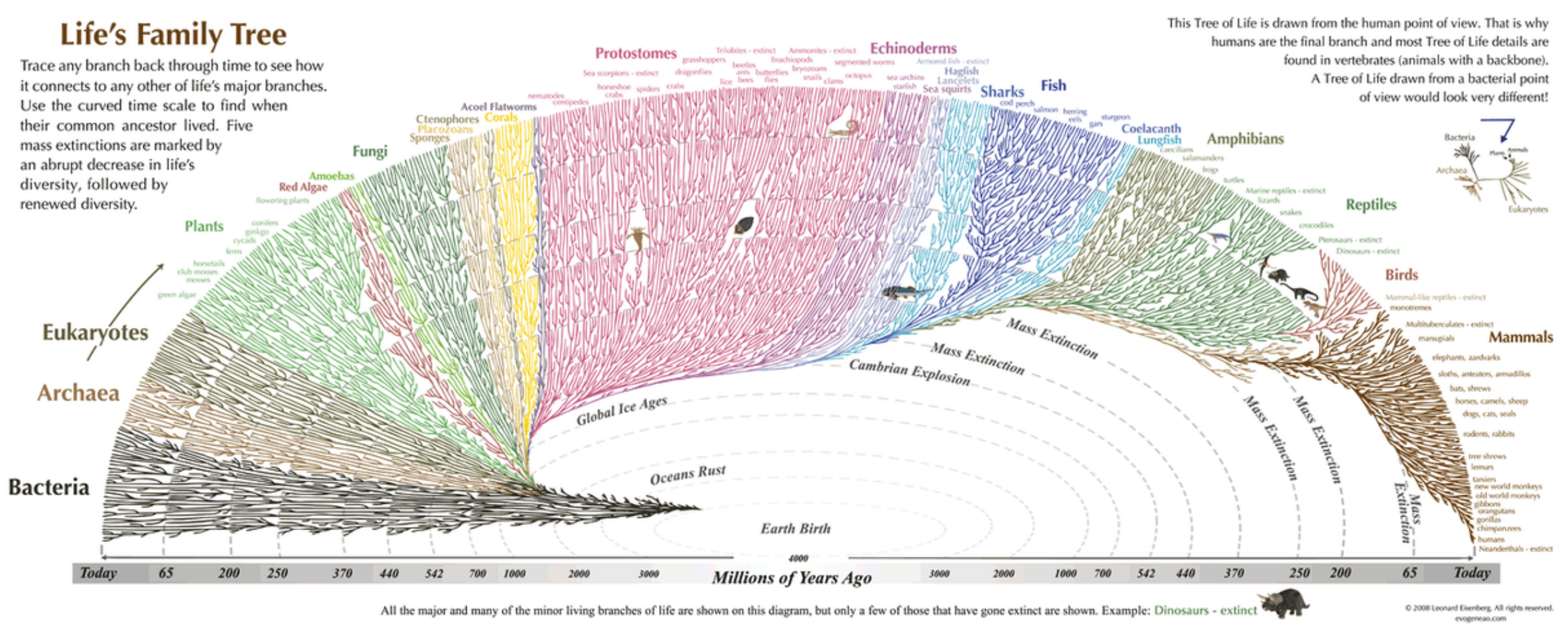
- 区块链的最重要的核心问题，就是如何解决公开网络上的信任问题，即无需信任的安全性。

- *不能把区块链作为万能的工具，什么都往区块链靠*
- *不能把区块链作为唯一的信任工具，现阶段是补充*

问题：区块链作为更好的工具，会成为唯一的工具吗？

人类需要什么样的区块链

“人类社会”是一个超级复杂的巨型系统



自古代帝国时代以来，社会的规模和相互依存度已经大大增加，整体复杂性也水涨船高。

再借用一下生物体的类比：社会原本就像是个非常简单的有机体（如微生物），现在已经演化成了更为复杂的有机体（如人类）。并且趋势还在继续，物理学理论告诉我们，所有系统的复杂性都会随时间的推移而增加。

协议共识无法脱离社会共识单独存在

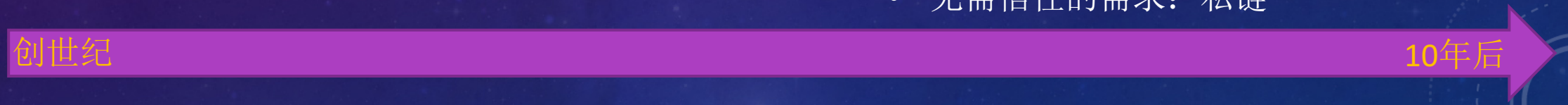
- Code is law？ETH分叉表明社区对结果正义和程序正义谁更重要有分歧。
- 协议共识的创立来自发起者的意志，其维护来自生态各方的参与。
- 其代表的人群所构建的社会共识是影响共识的根源。

启发：不仅区块链，其它初始在技术层面引发的竞争，随着发展最终会成为价值观的竞争。

没有应对所有需求的唯一解

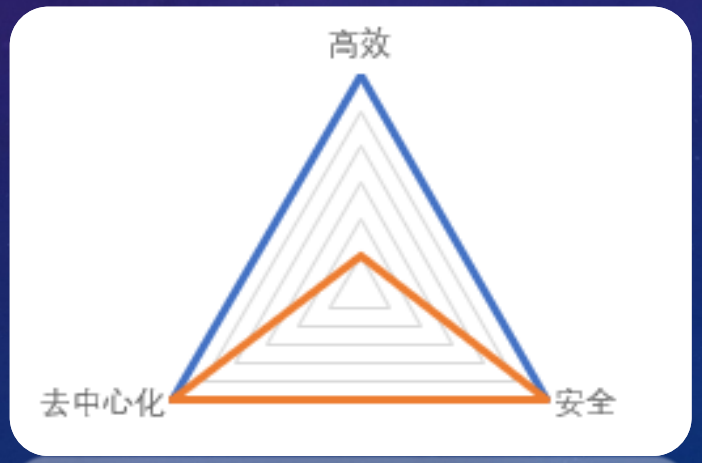
BTC点对点现金系统

- 高信任度的需求（货币）：BTC
- 较高信任度的需求（应用）：ETH
- 一般信任度的需求（应用）：EOS，联盟链
- 无需信任的需求：私链



区块链本身存在不可能三角

Decentralization —去中心化　无须依赖某个机构
Scalability —高效　每秒处理的交易笔数
Security —安全　难以篡改，保证数据安全和一致性



决定区块链特性的技术/功能

BTC： POW

ETH： 智能合约

EOS： DPOS

DFINITY： 可无限扩容

AELF： 跨链交互+性能提升

Cardano： POS

LOOM： 侧链

底层技术不断创新，目前对共识机制、中心化与去中心化、交易处理速度和安全等问题最为关注。

共识类型概览

网络环境的安全性

低

- POW
- POS

- DPOS
- BFT
- PAXOS/RAFT
- RPCA
- POOL

高

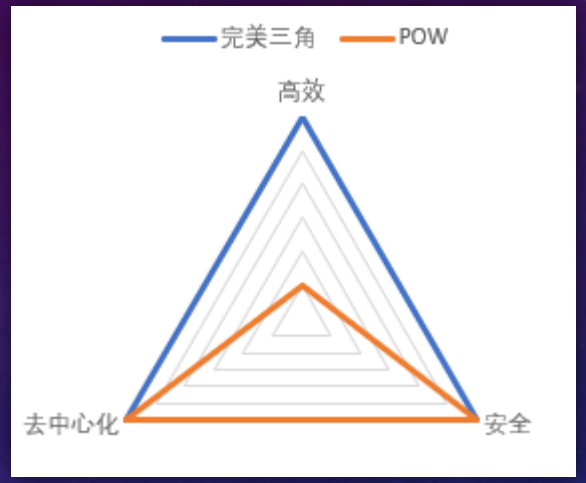
共识特点概览

共识算法	PoW	PoS	DPoS	RPCA	PAXOS	PBFT	RAFT	POOL
性能效率	低	较高	高	高	高	高	高	高
去中心化程度	完全	完全	半中心化	半中心化	半中心化	半中心化	半中心化	半中心化
最大允许作恶节点数量	50%	50%	50%	20%	50%	33%	50%	同选取的分布式一致性算法
是否需要代币	是	是	是	是	否	否	否	否
应用场景	公有链	公有链	公有链	私有链 联盟链	私有链 联盟链	私有链 联盟链	私有链 联盟链	私有链 联盟链
安全威胁	算力集中化	候选人作弊	候选人作弊	网关节点作弊	Proposer 节点故障	主节点故障	Leader 节点故障	同选取的分布式一致性算法
一致性	有分叉	有分叉	无分叉	无分叉	无分叉	无分叉	无分叉	无分叉
资源消耗	高	中	低	低	低	低	低	低
可监管性	弱	弱	弱	强	强	强	强	强

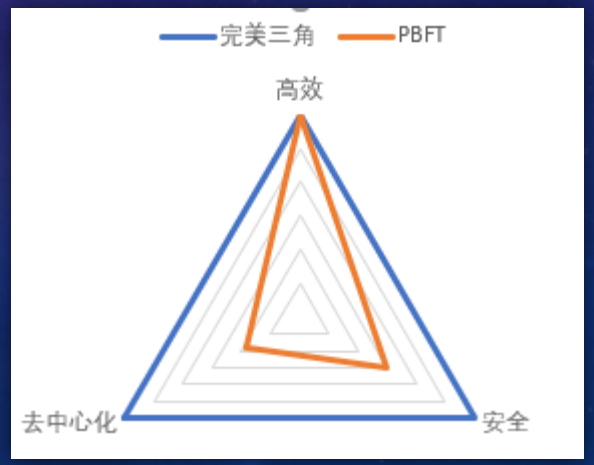
共识对比

- POW共识把系统的安全性交给了数学和能量消耗。
- POS共识把系统的安全性交给了人性的博弈。 Nothing-at-Stake attack； Long-range attacks； 马太效应

POS共识是虚拟世界中的一个封闭系统，如果共识的达成没有付出任何代价，共识的可靠性就可能存疑，人性博弈过程中的混乱一定会暴露出来。



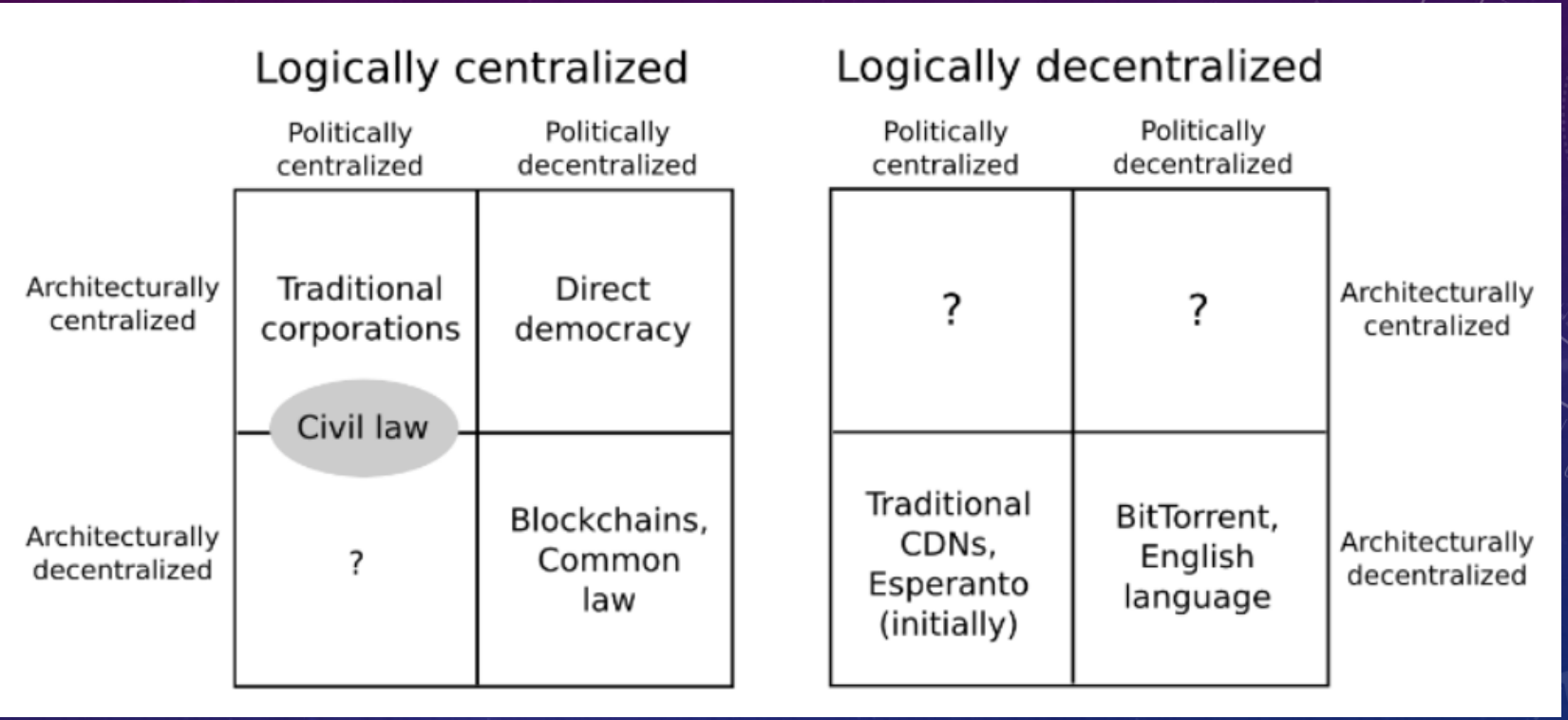
- DPOS：是为了效率而生的，它更加适用于对性能要求极高的相对封闭的商业系统。
- BFT：不超过1/3恶意节点，多节点时性能下降，且由于节点扩展性的缺陷，其共识节点的选择过程一样是封闭或者需要验证的，因而也更加适用于相对封闭的应用环境。



问题：

- POW的能耗是否是问题（军费）？
- 假如POW耗能更少，比特币网络会怎么样？
- 把无用计算变为有用计算从而不浪费是否可行？（随机，公平如何保证）

去中心化的维度



Vitalik Buterin：

当人们在讨论软件的去中心化时，他们实际上在讨论的，是三个独立的中心化/去中心化的轴。

- 架构上的（去）中心化—系统中物理计算机的数量来确定。任何时候，它能容忍崩溃电脑的数量越多，它就越去中心化。
- 政治上的（去）中心化—有多少的个人和组织能最终控制组成这个系统的电脑？
- 逻辑上的（去）中心化—系统呈现和维护的接口和数据库结构像是一个单一的整体呢？还是非结构群体？一个简单的启发是：如果你把这个系统的使用方和提供方一分为二，他们还能作为完全独立的单元进行运行吗？

区块链在政治上是去中心化的（没有人能控制），在架构体系上也是去中心化的（没有基础设施的中心故障点),但是在逻辑上是中心化的（有一个共同认可的状态，并且系统表现的像一个单一计算机）。

去中心化的目的

- 容错–去中心化系统不太可能因意外故障，因为它们依赖于许多独立组件，所以不太可能故障。
- 抗攻击–攻击和摧毁或操纵去中心化系统的成本更高，因为它们缺乏易受影响的中心点，而中心点的攻击成本比周围系统的要低得多。
- 抗合谋–去中心化系统的参与者难以互相勾结、合谋串通以牺牲其他参与者的利益为代价为自己谋利。

启发：

去中心化的目的是抗审查和安全

对审查的抵御足够了吗？对防篡保护到位了吗？谁有权利改变整个网络的规则？

隐私技术给人类以保护

“在我眼中，隐私就是让我们免于言行受到外界关注的困扰，并创造出一些空间以便我们为了自身的幸福而随心所欲地进行优化，只是为了我们自己的幸福，而不是因为在意别人对我们的看法。”—— Vitalik Buterin

- 隐私币；

Zcash ： zk-SNARKs 技术，该技术在使人们能够简洁且非交互性地证明自己知道某个信息的同时不透露具体内容。

Monero：环签名技术。正支持保护隐私的封包路由，用户可以隐藏自身地理位置和 IP 地址。

- 智能合约隐私；

代码全公开，如何保护用户隐私？Zether 、Keep 、Enigma、Origo 和 Covalent Oasis Labs 等正探索。

- 前沿研究：

主要涉及的主题有零知识、多方计算和全同态加密。后两者仍然处于理论阶段，实际运用时效率太低。

智能合约将是新经济的核心

Oliver Williamson和Ronald Coase（1991年诺贝尔经济学奖获得者）将合同置于经济和商业组织的核心。合约是制度密码经济学的核心。

- 合约越来越适合现实行业需要
- IBO STO 等应用的适用性将提升

公链的下一跳

- ✓高效
- ✓隐私
- ✓灵活

按真实需求设计和取舍特性

- 为什么比特币平均出块设定为10分钟？(分叉，交易分布）
- 为什么莱特币平均出块设定为2.5分钟？（广播+验证，1-2分钟）
- 为什么以太坊平均出块设定为12秒？（GHOST)

要预先考虑的问题：

需要多强的去中心化？需要多强的安全？

为多数人设计系统，还是为少数人设计系统？

为多数利益设计，还是为少数利益设计？

公链设计逻辑示例（VNS为例）

区块链源于密码朋克----回归初心

- 早期成员比如“维基解密”创始人Julian Assange、BT下载支付Bram Cohen、万维网发明者Tim Berners-Lee、智能合约概念提出者Nick Szabo、Facebook创始人之一Sean Parker、中本聪等。
- 提倡大规模使用强加密算法来保护自身基本自由免受攻击，同时反对任何政府规则的密码系统。
- 在比特币出现之前，密码朋克内成员至少讨论及发表过十种以上类似的数字货币及支付系统，比如E-cash、B-money，不过这些货币大都以失败告终。

- 思考点：
- 1 密码朋克的主张缘由及影响是什么？
- 2 BTC之前的数字货币为什么失败？

区块链依赖于现实世界----依托现实

比特币为例：

设计逻辑的依赖：

I. 参与者群体：中本聪同学说，只要挖矿组织中大多数人是诚实的，这个系统就可靠

II. 密码学：从概率上保证安全

III. 共识算法：从概率上保证安全

部署实施的依赖:

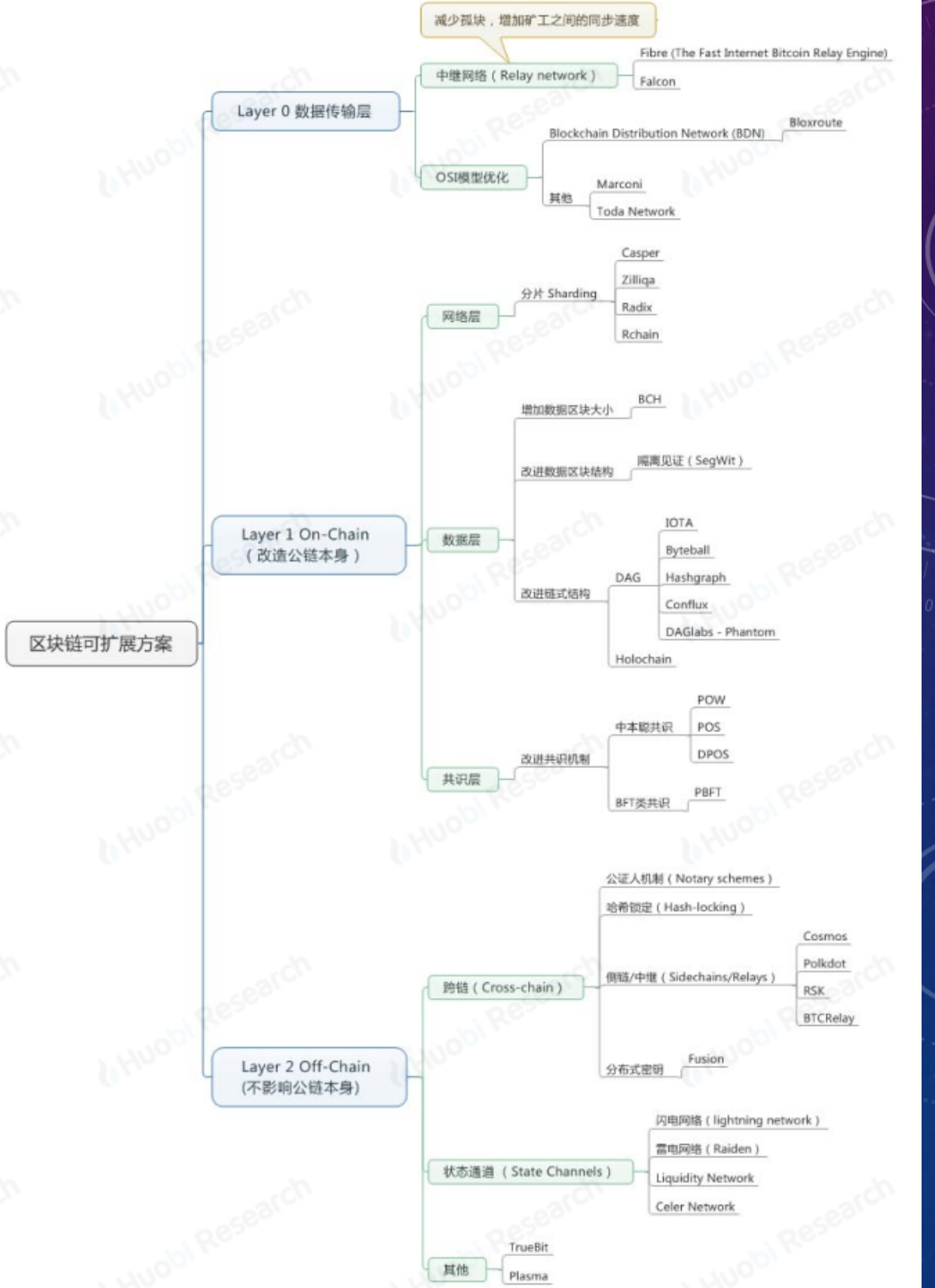
I. 极客和公众的认知水平

II. 去中心化未成形时外部对立力量介入程度（棱镜调查，Wiki解密捐助事件）

让区块链干它该干的事情----安全稳妥

扩容方案选择----积极创新，兼容并蓄

- ✓独创POW+POS
- ✓其它方案互补



关键设定和目前状态

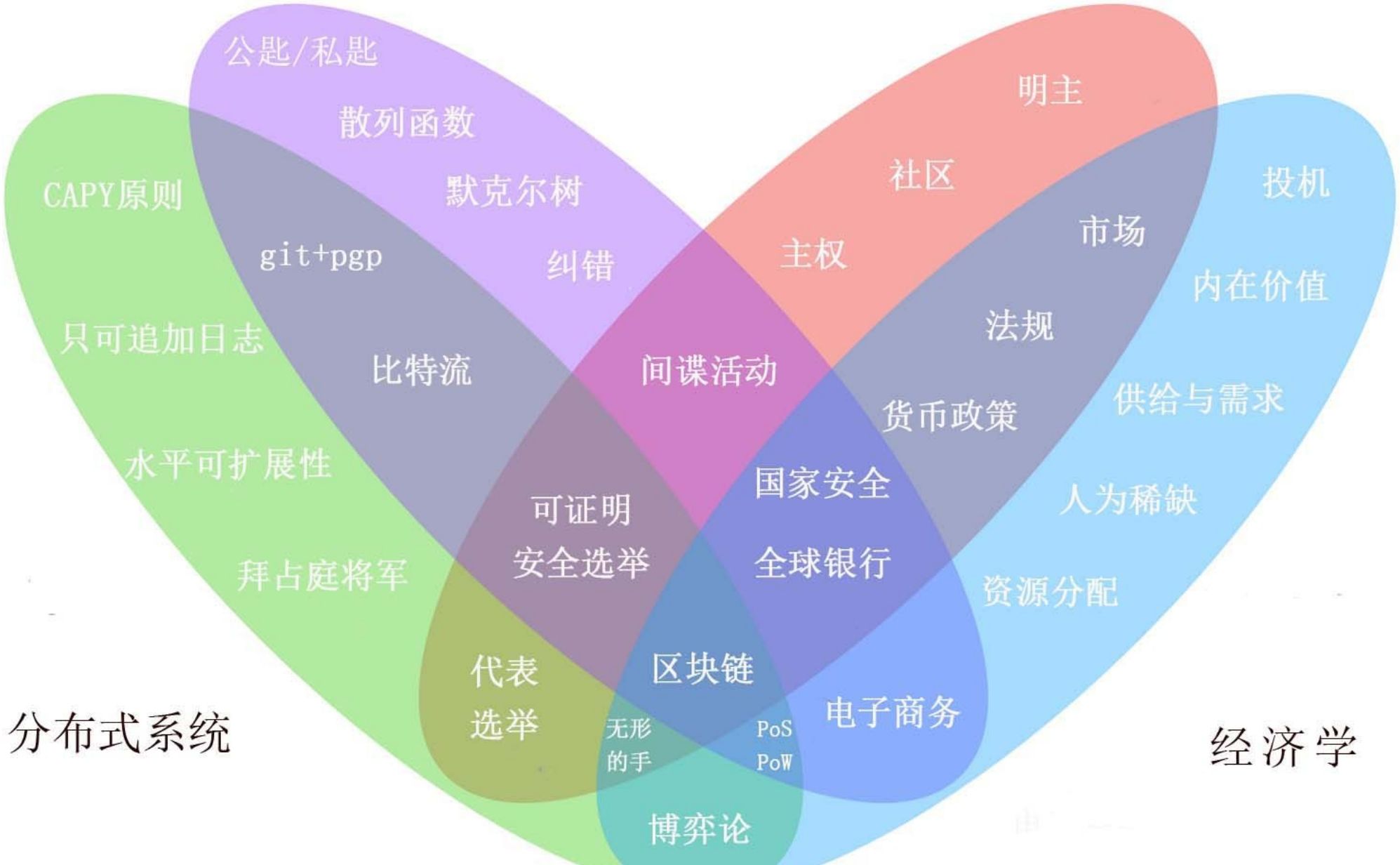
- 最低硬件门槛的参与方式：亲cpu算法，废旧电脑都可以建立pow节点-----最大限度的生存性
- 最低脑力门槛的参与方式：一键挖矿，超级省心，同时办公游戏无影响。 人人可参与-----最大范围平等、公平地参与
- 100年出块：保证网络持久发展
- POW+POS：权衡多方诉求
- 支持智能合约：贴合实体经济需求
- 支持Bancor：提供经济设计的灵活性
- 创始人退出计划：自我约束，依规治理

- ✓ 主网上线200天，用户，算力等关键指标稳步提升
- ✓ 500+种token
- ✓ 圈外应用：实体企业对接，小程序合作，游戏接入。
- ✓ 独立行情
- ✓ 多生态方支持

我们真正面临的选择是：

THE RIGHT WAY, OR THE EASY WAY. （正确的，还是容易的）

区块链光谱


密码学
政治学
公匙/私匙
散列函数
默克尔树
CAPY原则
git+pgp
纠错
只可追加日志
比特流
水平可扩展性
拜占庭将军
明主
社区
投机
市场
主权
内在价值
法规
间谍活动
供给与需求
货币政策
国家安全
人为稀缺
可证明
安全选举
全球银行
资源分配
代表
选举
区块链
电子商务
无形
的手
PoS
PoW
博弈论
分布式系统
经济学

VNS, 不仅仅是技术上的公链----发展十问

- 实体经济转型通证经济，权益碎片化如何解决？（公权力和私权的边界）
- 如何平衡可度量的贡献和不可量化的贡献以防止激励让社区扭曲？
- 考虑到现实世界的情况，区块链系统规模多大较好？如果越大越好，越大越稳定，那BTC分裂出BCH，BCH又分裂出BSV好吗？
- 系统越大，涵盖的参与者越多，牵扯的利益越多（程度和种类都增多），问题：10个人组成一个系统，两种情况：1 意见趋同 2有两种意见 ；前者内部稳定，后者对外部适应性好。哪种情况下系统更稳定，更有发展？
- 主流的通货膨胀的经济政策是否合理？公链应该如何设定？
- 有效的货币制度，需要有效的监管，如何在制度上实现有效监管？（进一步看，美联储产生的原因是因为什么？）
- 单中心国家秩序支撑的货币政策，实际上让市场自身失去自我调整的功能，从而创造了危机，而且还进一步放大了危机。对公链有什么启发？
- 全球性金融和国家主权的矛盾，特殊利益政治的矛盾，意识形态的矛盾等，将如何影响公链的发展？
- 如何应对黑天鹅，实现反脆弱？
- 工业革命出现在一个商业模式以等级制度和金融资本主义为根据的世界里。区块链革命将会见证一个由人力资本主义和高度自治为主导的经济体制。新的规则如何建立，有比代议制，三权分立等更好的吗？

黄色的树林里分出两条路，
可惜我不能同时去涉足，
我在那路口久久伫立，
我向着一条路极目望去，
直到它消失在丛林深处。

但我却选了另外一条路，
它荒草萋萋，十分幽寂，
显得更诱人，更美丽；
虽然在这条小路上，
很少留下旅人的足迹。

那天清晨落叶满地，
两条路都未经脚步污染。
啊，留下一条路等改日再见！
但我知道路径延绵无尽头，
恐怕我难以再回返。

也许多少年后在某个地方，
我将轻声叹息把往事回顾：
一片树林里分出两条路——
而我选择了人迹更少的一条，
从此决定了我一生的道路。

送给每一个正穿越凛冬，走在选择路上的人