新型数据库-区块链

币看·深圳数字奇点科技有限公司 CEO 刘洋

自我介绍

1995-1999年大连理工大学计算机科学与工程专业毕业

2000-2014年华为技术有限公司，从技术到管理（研发总监）

2014-至今，联合创立“币看比特币”并出任CEO

刘洋

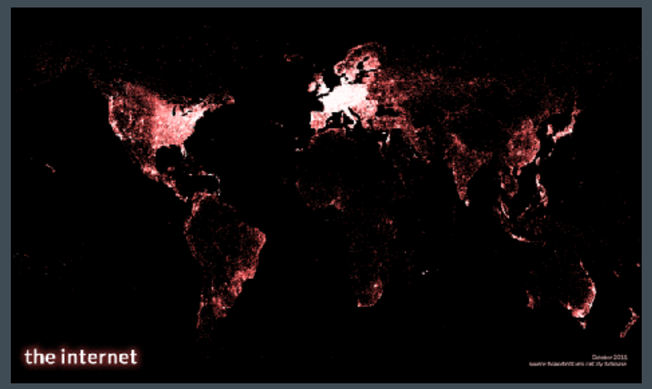
联合创始人&CEO

币看是集行情、资讯、挖矿、钱包和交易为一体的加密数字货币服务平台

BITKAN

信息技术第三次革命

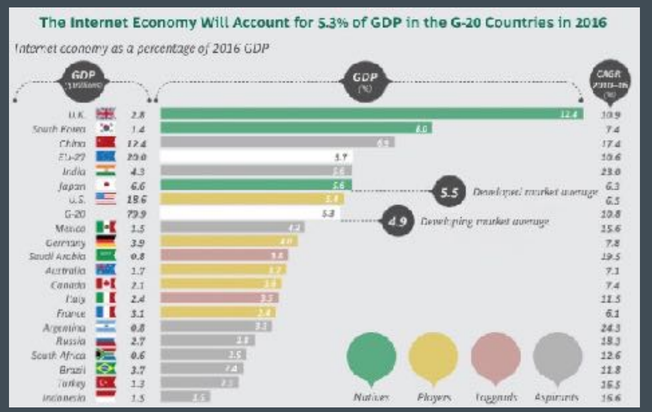
互联网社会



互联网人口

47%

2016年世界人口73亿，接入互联网的人口达47%



互联网经济

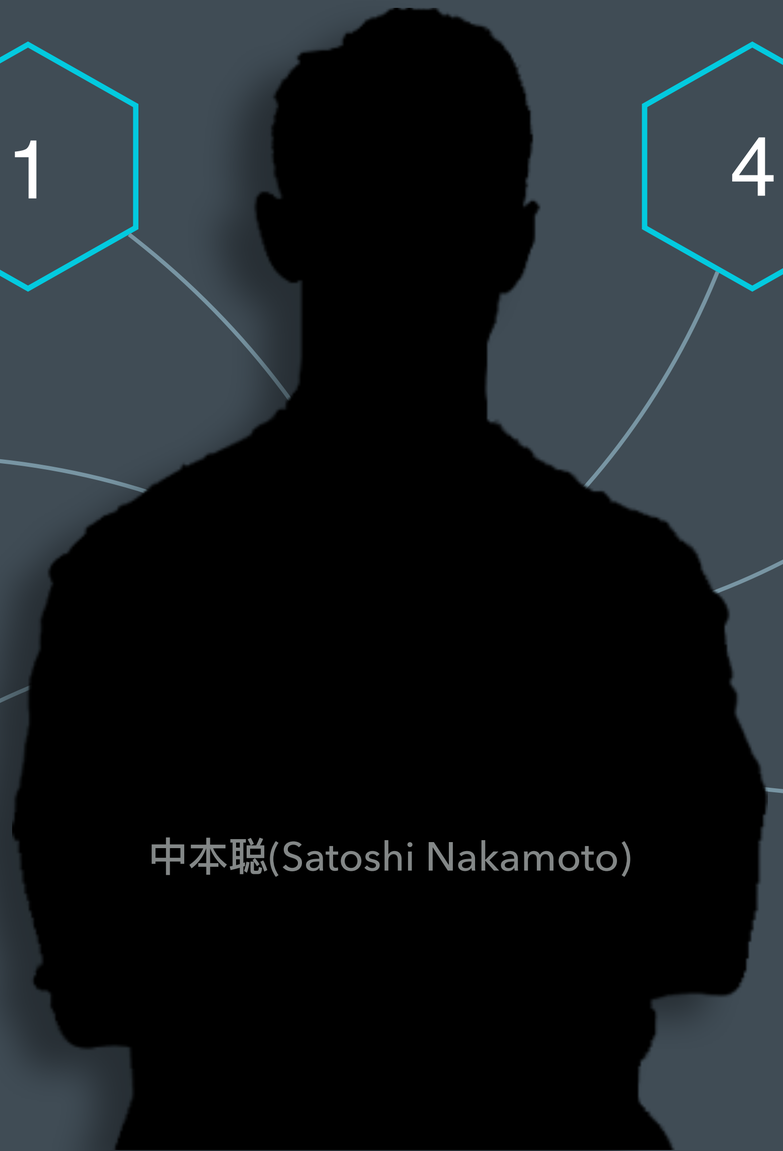
5.3%

G20国家的互联网经济占比GDP 5.3%，其中中国互联网经济占国家GDP的17.4%

互联网社会缺少信用基础

数据来源-维基百科2016年

比特币发展简史



1

白皮书

2008年10月发布白皮书

2

创世纪块

2009年1月发布软件版本并挖出第一个区块（50BTC）

3

比特币披萨节

2010年5月21人，一个程序员用1万个BTC购买一个披萨

4

交易平台

2010年7月第一家交易平台Mt.Gox上线

5

丝绸之路

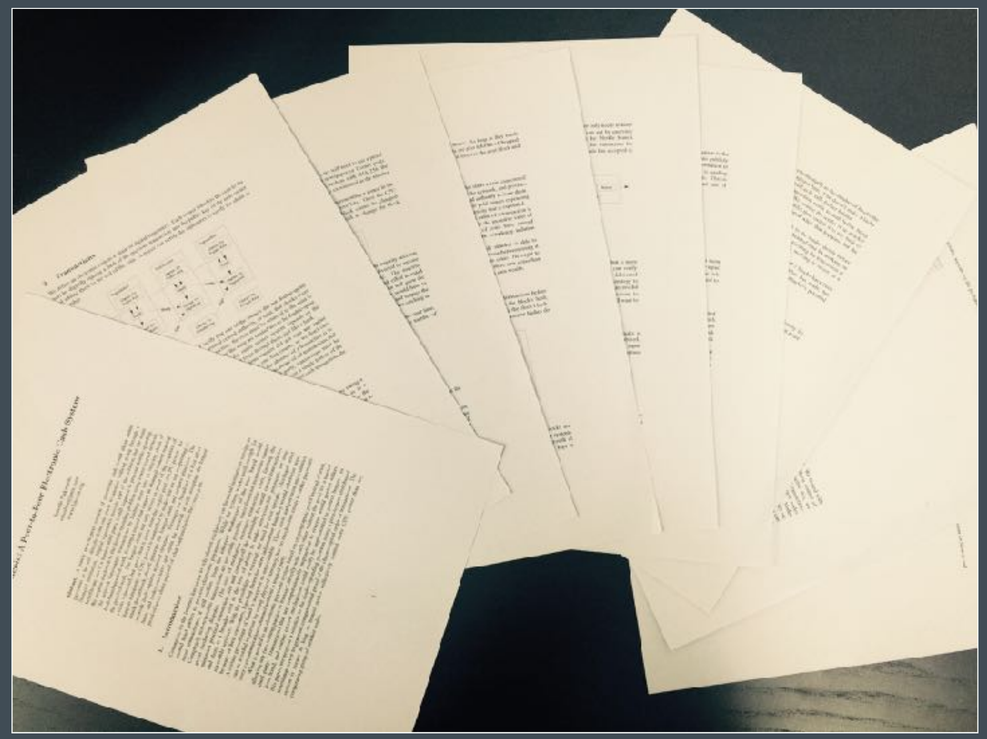
2011年2月，丝绸之路（黑市网站）上线，只接受比特币

6

央行表态

2013年12月5日，央行联合五部委发布《关于防范比特币风险的通知》

一种点对点的现金系统



https://bitcoin.org/en/bitcoin-paper

9页论文纸

3万行C++代码

3个月从论文到上线

定义比特币

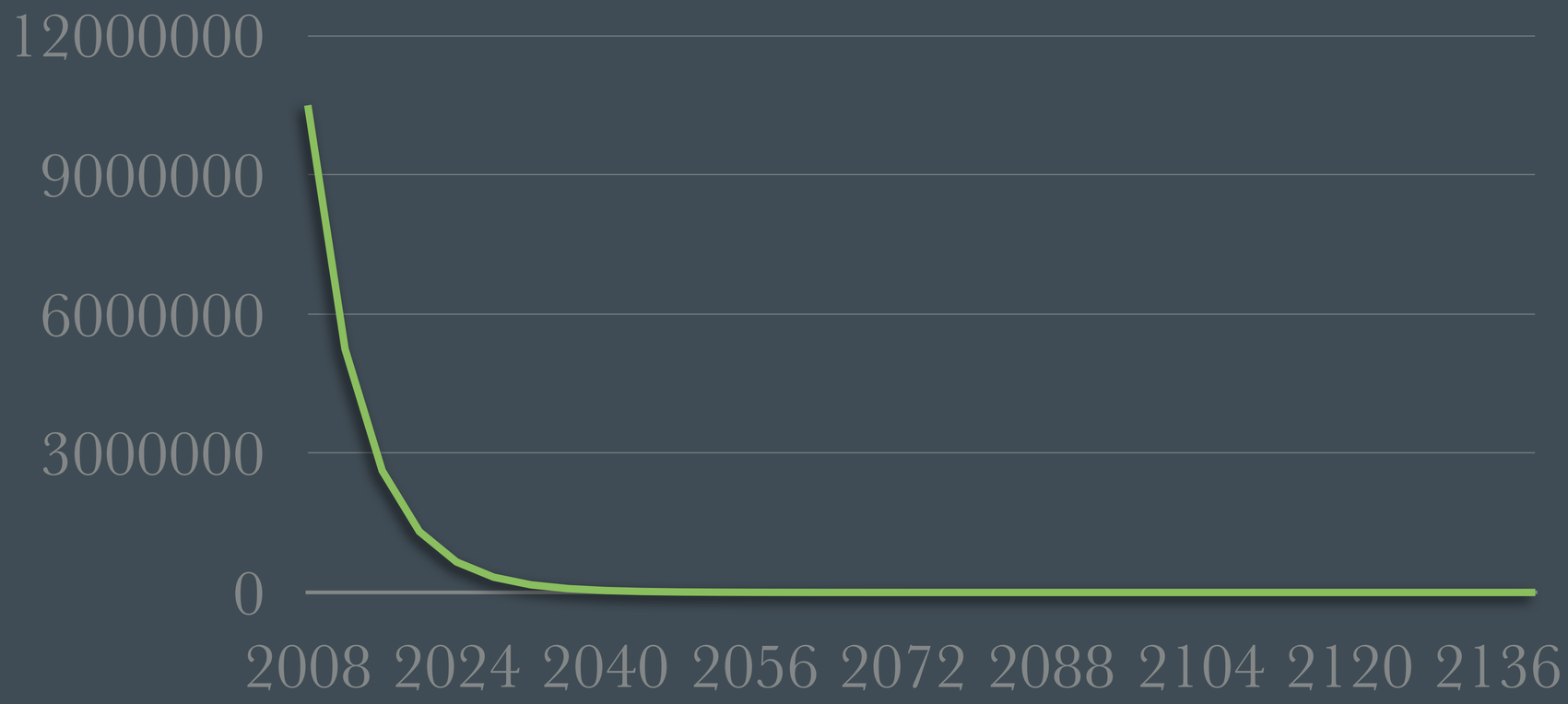
总量2100万个

发行速度

价值低 → 价值高

早期快 → 后期慢

$$\sum_{n=0}^{29} 50 * 0.5^n * 210000$$



50

埋起来：630万个箱子，21万个50个(空头支票)装，21万个25个装。。。

BITKAN

发行周期

控制速度,10分钟找到一个

计 算 困 难 ， 检 验 容 易

出题

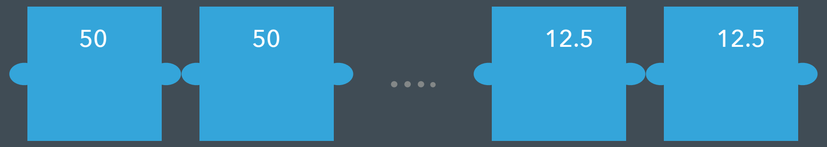
掷骰子（SHA256结果为64字节），先计算出结果小于目标值的，获得该块的奖励

难度调整

每2016次(大约14天)调整一次难度，控制节奏在10分钟左右

算题者

算题的就是矿机，过程就是挖矿（POW），无主的奖励标记为所有权为自己



转账

比特币实际是支票形式

类似于支票的转账单

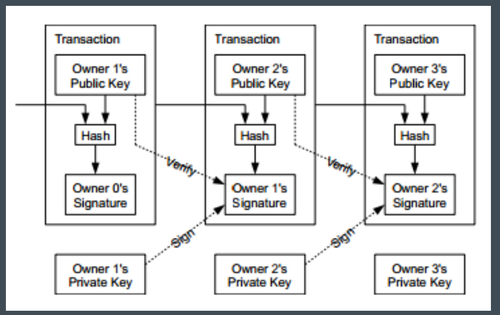
从哪个转账单转出多少个比特币到目标地址，出示的签名

记账

第一个发现块的节点检验转账的有效性并将转账记录在发现的块上广播出去

转账单

所有的转账单一旦使用必须被花费掉，剩余部分转给自己再生成一张转账单



手续费

转账的入和-出和的金额就是手续费，由矿工（第一个发现块的节点）加在奖励币标识为自己拥有

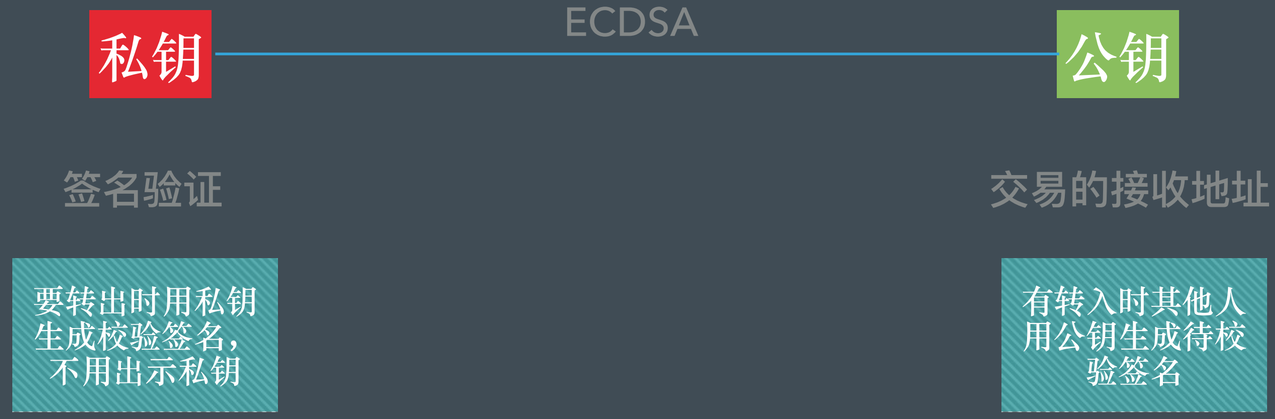
接收地址，转出签名

非对称加密

ECDSA，一对公私钥，私钥签名公钥验证

用途

公钥用来做接收的地址，转出时出示私钥签名



防伪机制

不易被篡改，容灾能力强

分布式存储

通过广播（8333）通知所有节点，每个节点一个相同的拷贝，
防伪的同时提高容灾

验证真伪

通过HASH和MERKLE根等技术可以非常容易的验证真伪，从
而防伪

共识机制

分布式存储+POW共同组成了强壮的共识机制

比特币是什么

全球唯一的链式账本

分布式

不存在中心的服务器节点，所有节点都是对等的，并拥有相同的账本拷贝，运行着相同的软件系统

记账模式

不存在比特币的实体，只是记录着转移比特币的源、目标和数量等交易信息

区块链

每一个箱子就叫一个区块（Block），以链式（Chain）存储，技术名称“区块链技术”

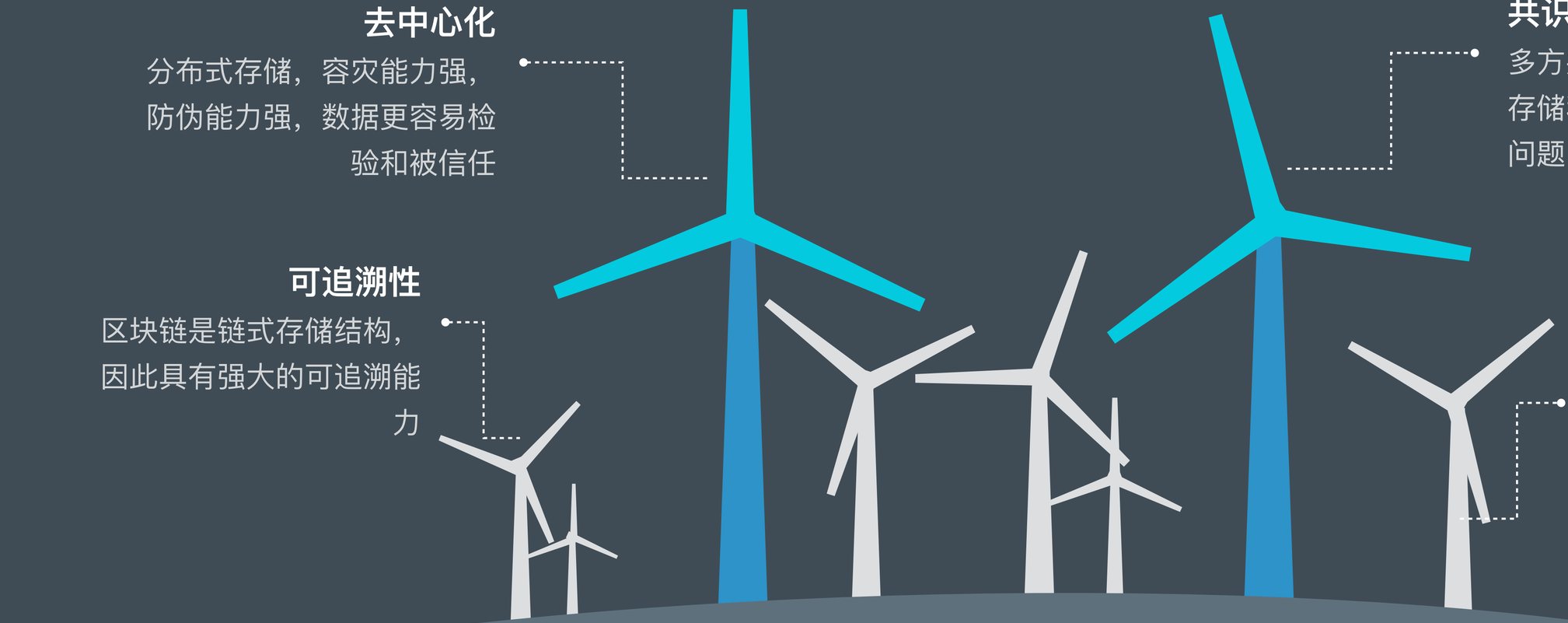
区块链是什么

去中心化

分布式存储，容灾能力强，防伪能力强，数据更容易检验和被信任

可追溯性

区块链是链式存储结构，因此具有强大的可追溯能力



共识机制

多方共同参与区块链数据的存储和校验，可解决互信的问题

不可篡改

区块链一经写入便不可篡改，校验机制确保去伪存真

实现比特币的底层技术

区块链应用的三大误区

原始数据造假

区块链应用写入的数据如何保障是真实有效的?

POW/POS

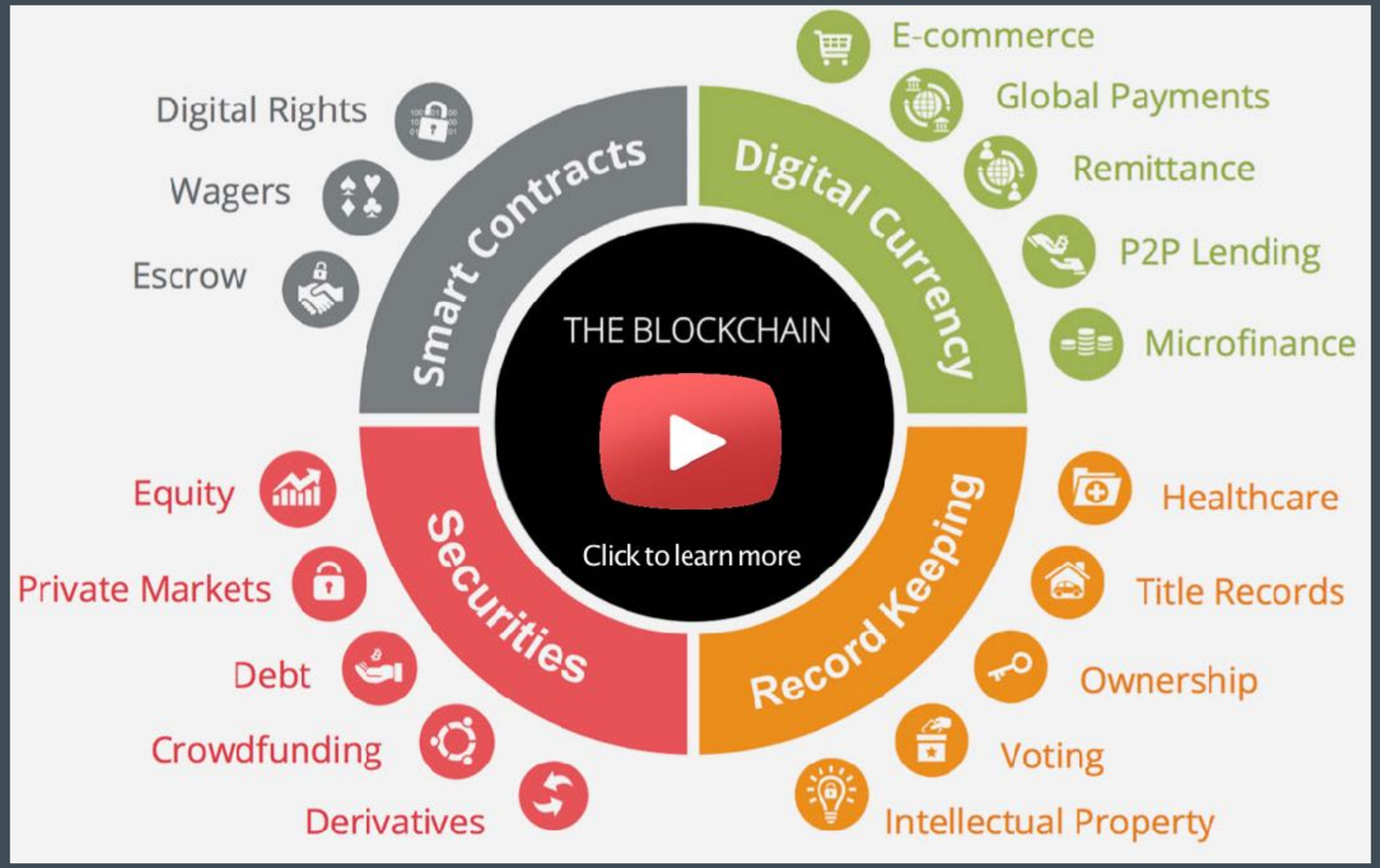
如果是POW如何获取大量的算力（重复建设），POS如何确保联盟不造假

平台应用

区块链是技术不是服务，走平台服务这条路谁来买单?

手里拿着锤子，看什么都是钉子，区块链技术还有一段相当长的路要走...

区块链可能的应用领域



区块链存储的数据应当量小且价值大

谢 谢

区块链技术构筑了信用价值网络

BITKAN