SDCC 2016

中国软件开发者大会

SOFTWARE DEVELOPER CONFERENCE CHINA

区块链和分布式数据库

Blockchain and Distributed Database

Raymond@CarelessWhisper

640K对所有人都够了

640K ought to be enough for anybody.

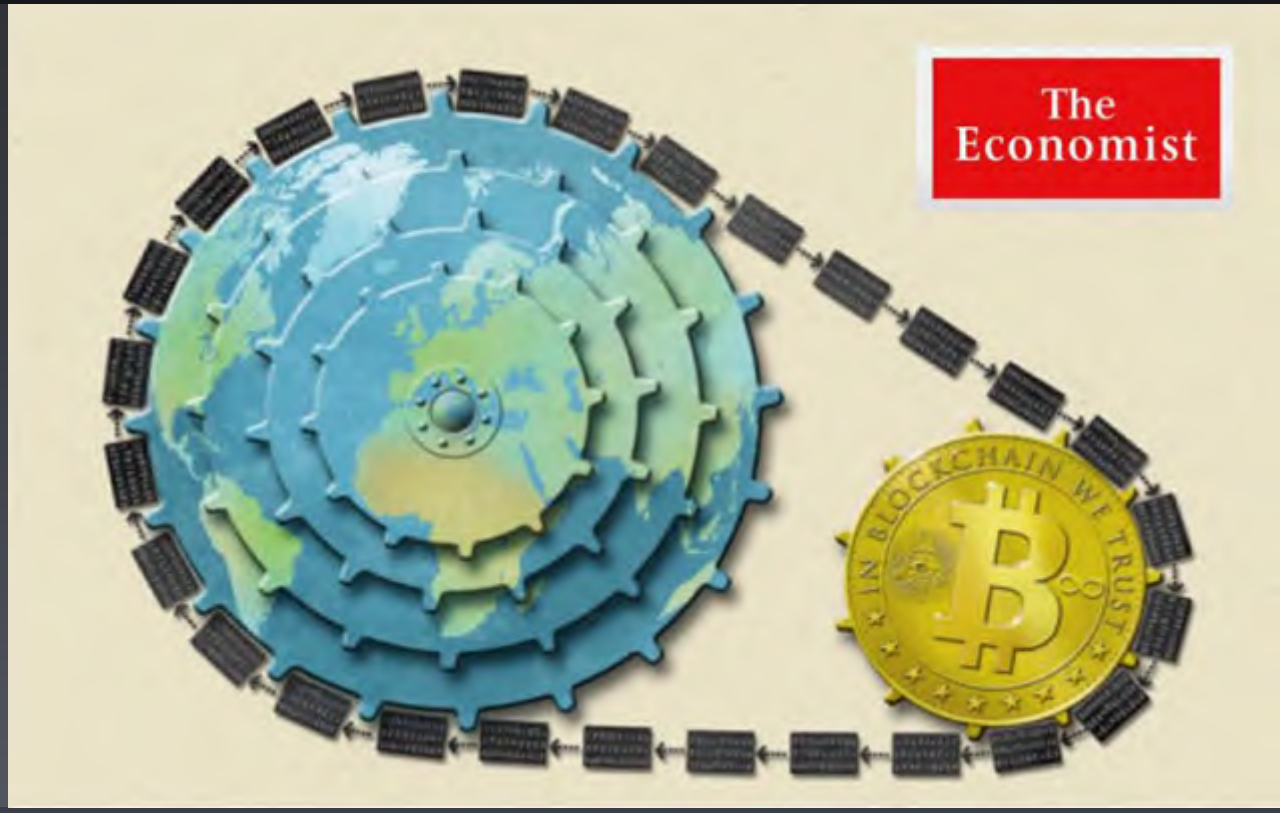
From the dawn of civilization until 2003, humankind generated five exabytes of data. Now we produce five exabytes every two days...and the pace is accelerating.

Eric Schmidt,
Executive Chairman, Google

核心就是数据

The trust machine
The promise of the blockchain

The technology behind bitcoin could transform how the economy works



区块链是一个复杂的概念

The first five times you think you understand it, you don't.

What color is your blockchain?

比特币背后的区块链

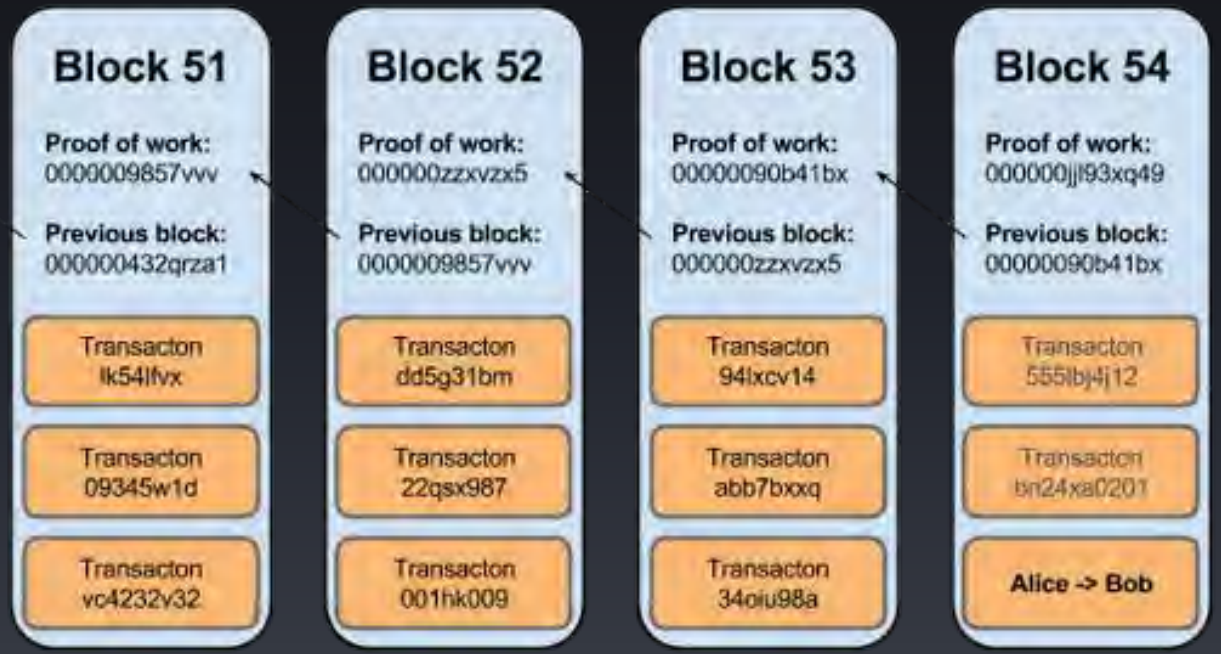
Bitcoin Whitepaper by Satoshi Nakamoto

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.

区块链就是区块的链


Block 51
Proof of work:
0000009857vvv
Previous block:
000000432qrza1
Transacton
lk54lfvx
Transacton
09345w1d
Transacton
vc4232v32
Block 52
Proof of work:
000000zzxvzx5
Previous block:
0000009857vvv
Transacton
dd5g31bm
Transacton
22qsx987
Transacton
001hk009
Block 53
Proof of work:
00000090b41bx
Previous block:
000000zzxvzx5
Transacton
94lxcv14
Transacton
abb7bxxq
Transacton
34oiu98a
Block 54
Proof of work:
000000jjl93xq49
Previous block:
00000090b41bx
Transacton
555lbj4j12
Transacton
bn24xa0201
Alice -> Bob

THE TIMES
Eat Out from £5
Israel prepares to send tanks and troops into Gaza
Chancellor on brink of second bailout for banks

创世区块

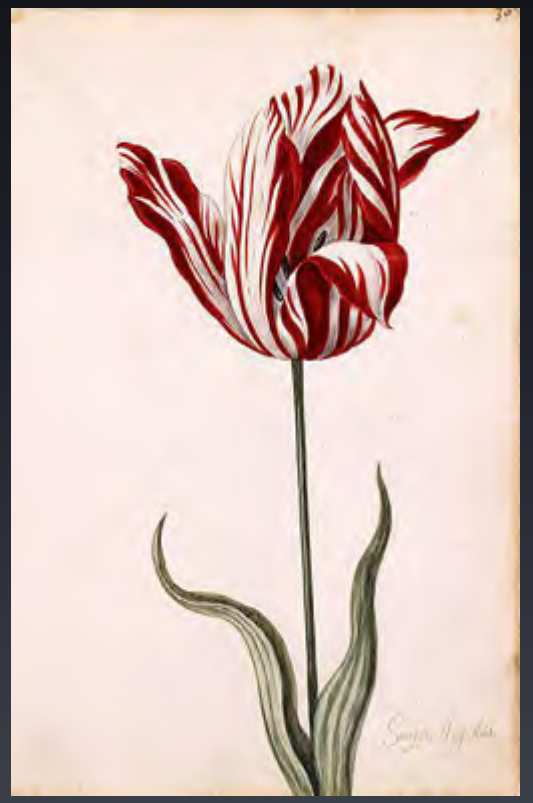
可以无限分割的货币

- 1mBTC = 0.001BTC
- 1Satoshi=0.000001BTC
- 1 mBTC = ~$0.40
- 1 Satoshi = ~$0.0004

不可以随意产生的币

- 不是花了钱就有新的比特币
- 没有中央银行
- 程序员每次只能挖出固定数量的币
- 无法应市场要求加快或者加大量产

两个
常用的对比



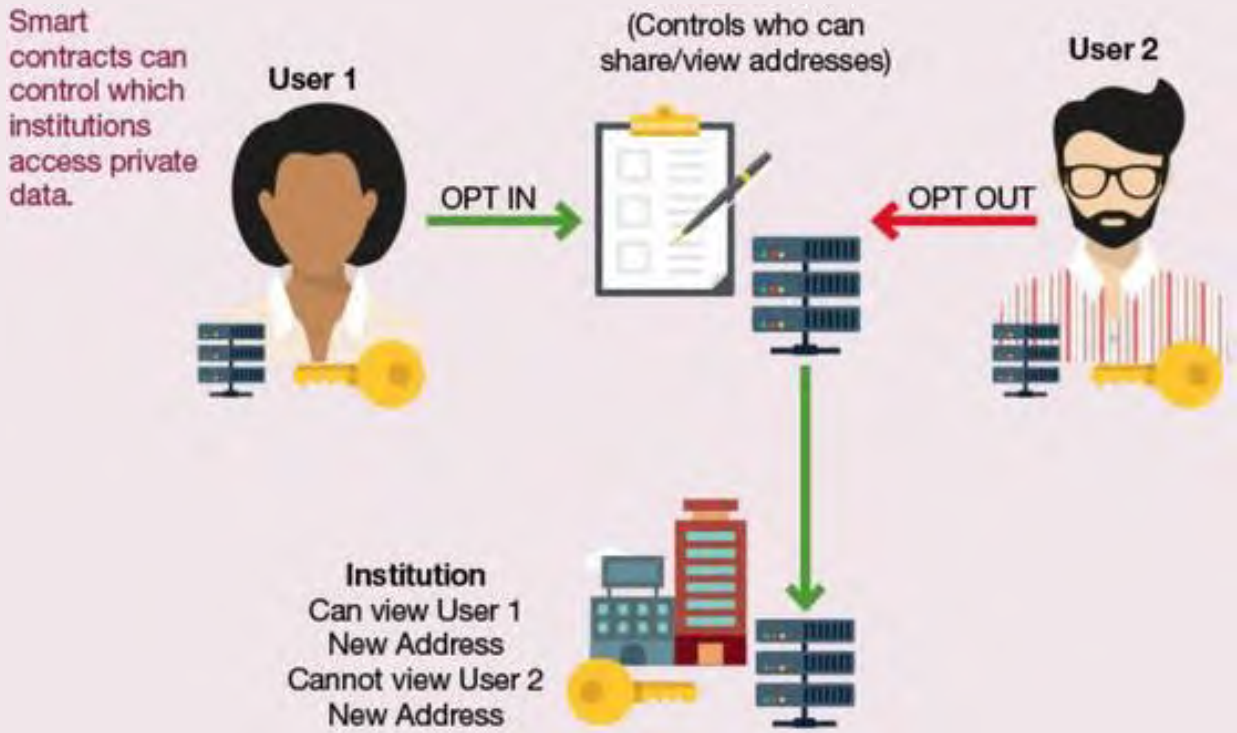
Alice
(Public)
10 BTC
Bob
(Public)
0.2 BTC
Charlie
(Public)
17 BTC
Dora
(Public)
0.001 BTC
Eliza
(Public)
2 BTC

智能合约

智能合约是什么

账户名	股票	资金
Peter	100股Facebook	0
Jeff	0	$4,000

账户名	股票	资金
Peter	60股Facebook	$4,000
Jeff	40股Facebook	$0


Smart contracts can control which institutions access private data.
User 1
(Controls who can share/view addresses)
User 2
OPT IN
OPT OUT
Institution
Can view User 1 New Address
Cannot view User 2 New Address

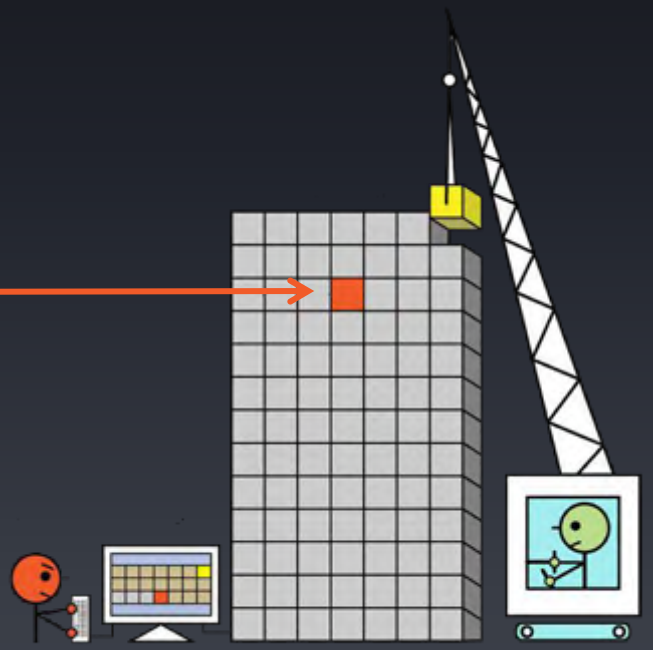
智能合约

区块链系统的不可篡改性

Why You Can't Cheat at Bitcoin

1.Say everybody is working on **block 91**.

2.But one miner wants to alter a transaction in block 74



3.He'd have to make his changes and redo all the computations for blocks 74-90 and do block 91.That's **18 blocks of expensive computing**

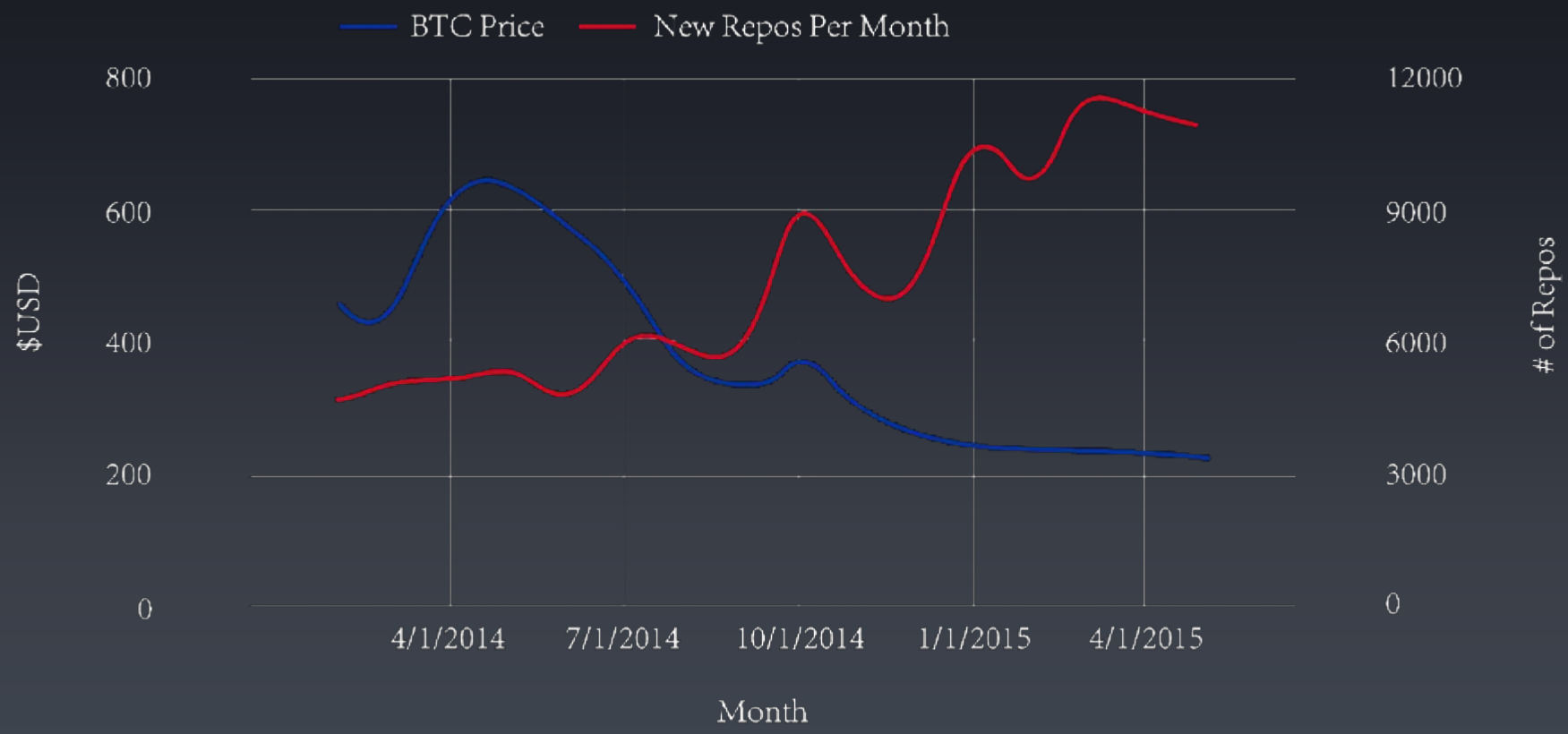
4.What's worse,he'd have to do it all **before** everybody else in the Bitcoin network finished **just the one block(number 91)**that they're working on.

被机器人取代的十个行业

比特币，区块链1.0

区块链2.0

代码库数量和比特币价格对比

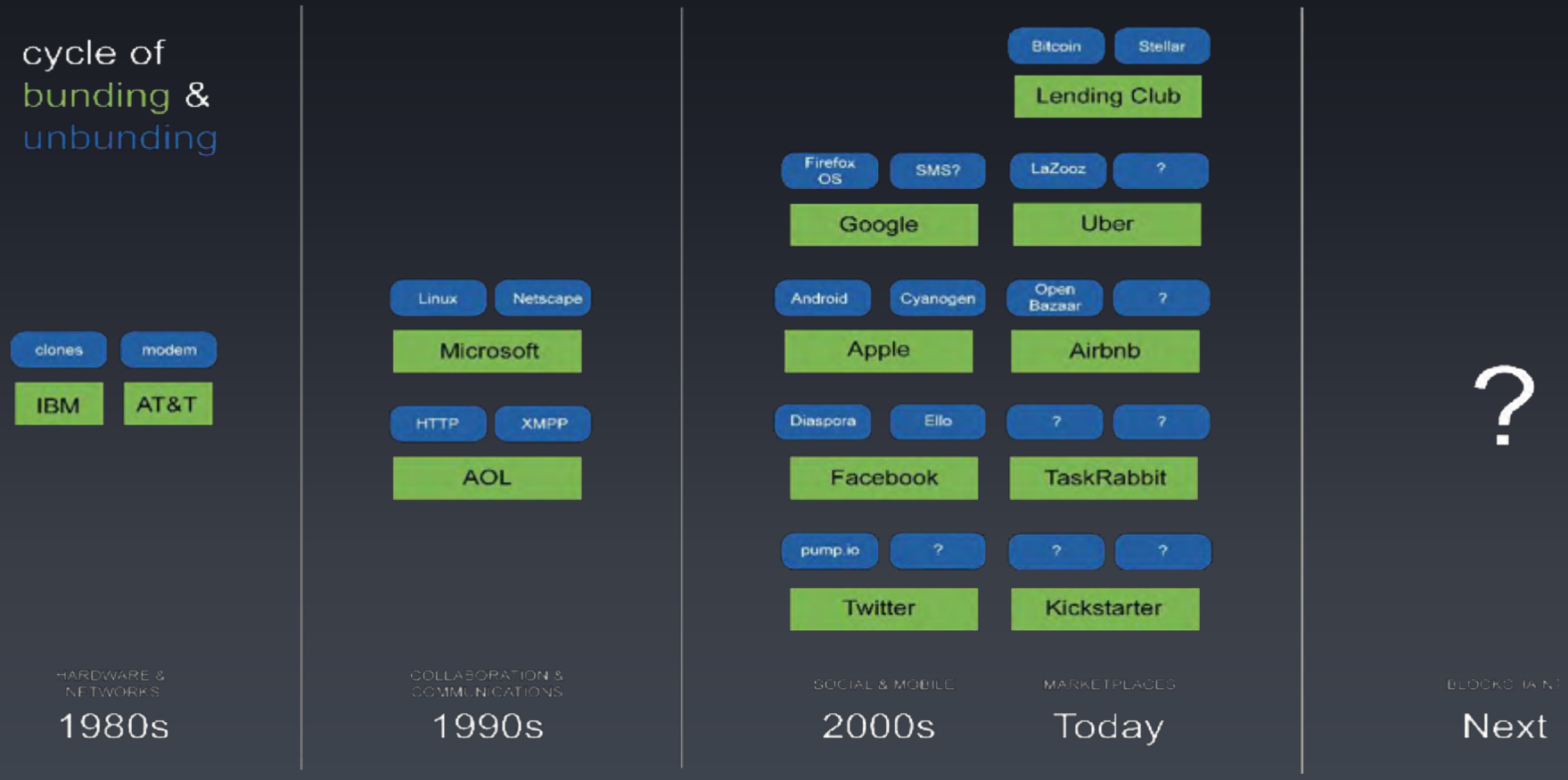


区块链

- Distributed（分布式的）
- Autonomous（自治的，共同约定的）
- Contractual（按照合约执行的）
- Trackable（可追溯的）

分布式账本

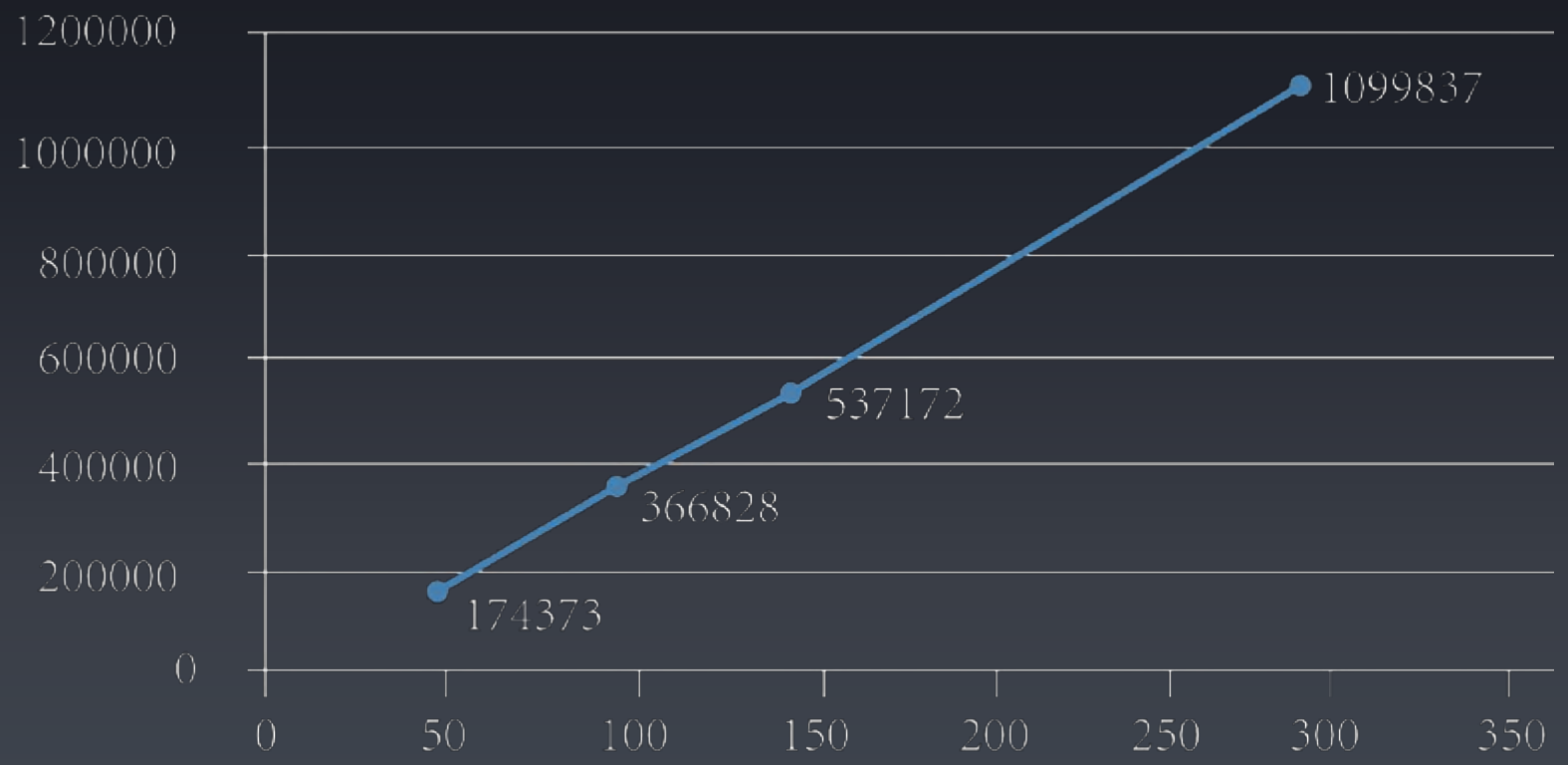
信息技术的五次变革


cycle of
bunding &
unbunding
clones
modem
IBM
AT&T
HARDWARE & NETWORKS
1980s
Linux
Netscape
Microsoft
HTTP
XMPP
AOL
COLLABORATION & COMMUNICATIONS
1990s
Bitcoin
Stellar
Lending Club
Firefox OS
SMS?
LaZooz
?
Google
Uber
Android
Cyanogen
Open Bazaar
?
Apple
Airbnb
Diaspora
Ello
?
?
Facebook
TaskRabbit
pump.io
?
?
?
Twitter
Kickstarter
SOCIAL & MOBILE
MARKETPLACES
2000s
Today
?
Next

大数据和区块链的结合

- 大数据的区块链化
- 区块链的大数据化

分布式数据库的可延展性（write/s）



三层架构

区块链业务应用层

区块链引擎层

分布式数据库存储层

Big Data 框架

Data Ingestion
Manipulation
Integration

Enterprise &
Ad Hoc
Reporting

Data
Discovery
Visualization

Predictive Analytics

Big Data Analytics

Hadoop

Blockchain

Analytic
Databases

RDBMS

SDCC 2016

中国软件开发者大会

SOFTWARE DEVELOPER CONFERENCE CHINA

感谢聆听

@CarelessWhisper