区块链技术

—— 通往未来的虫洞

达鸿飞

小蚁 创始人/CEO

2015.8.9 上海对外经贸大学

Contents

1 区块链

2 区块链技术

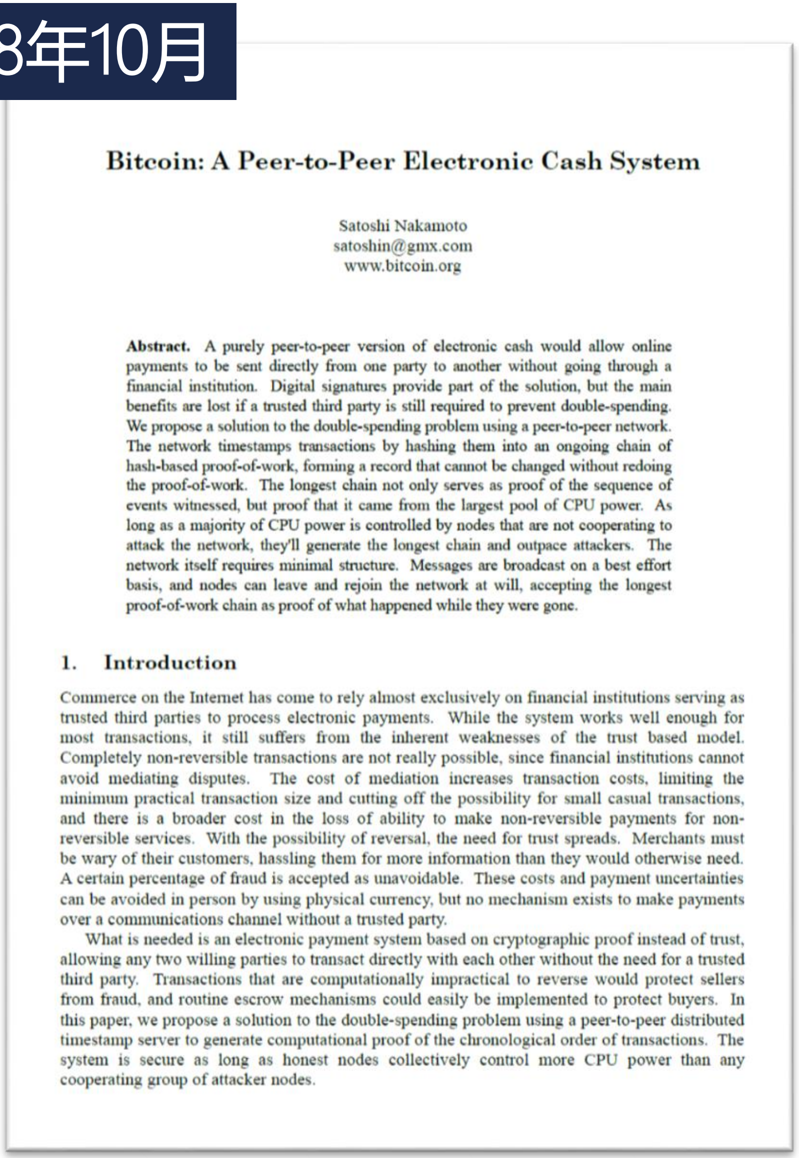
3 区块链与未来

Contents

1 区块链

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

2008年10月



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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

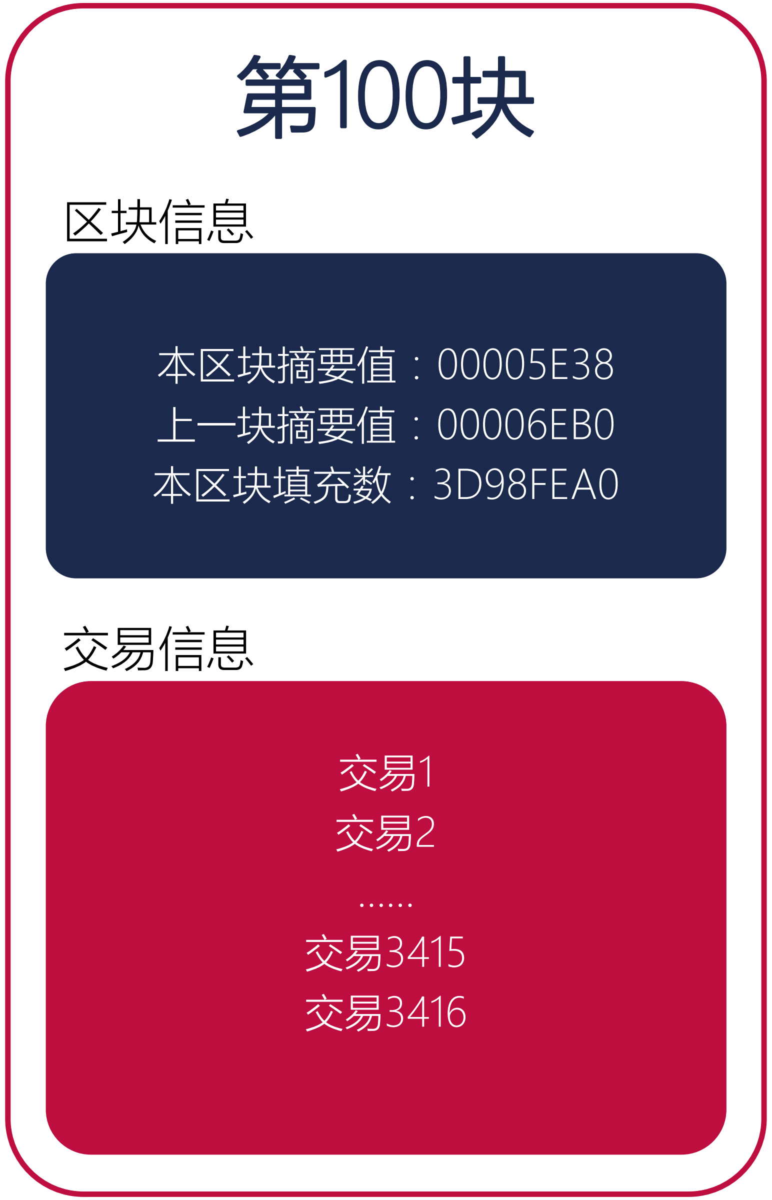
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

A 2008年，中本聪发表了《比特币：一种点对点的电子现金系统》白皮书

B 白皮书内并没有直接提到blockchain、block chain、chain of blocks

C 时至今日（2015.8），比特币的数据目录大小接近50GB

D 比特币市值240亿人民币，经受住了无数黑客的攻击，区块链的安全性得到了验证



第100块

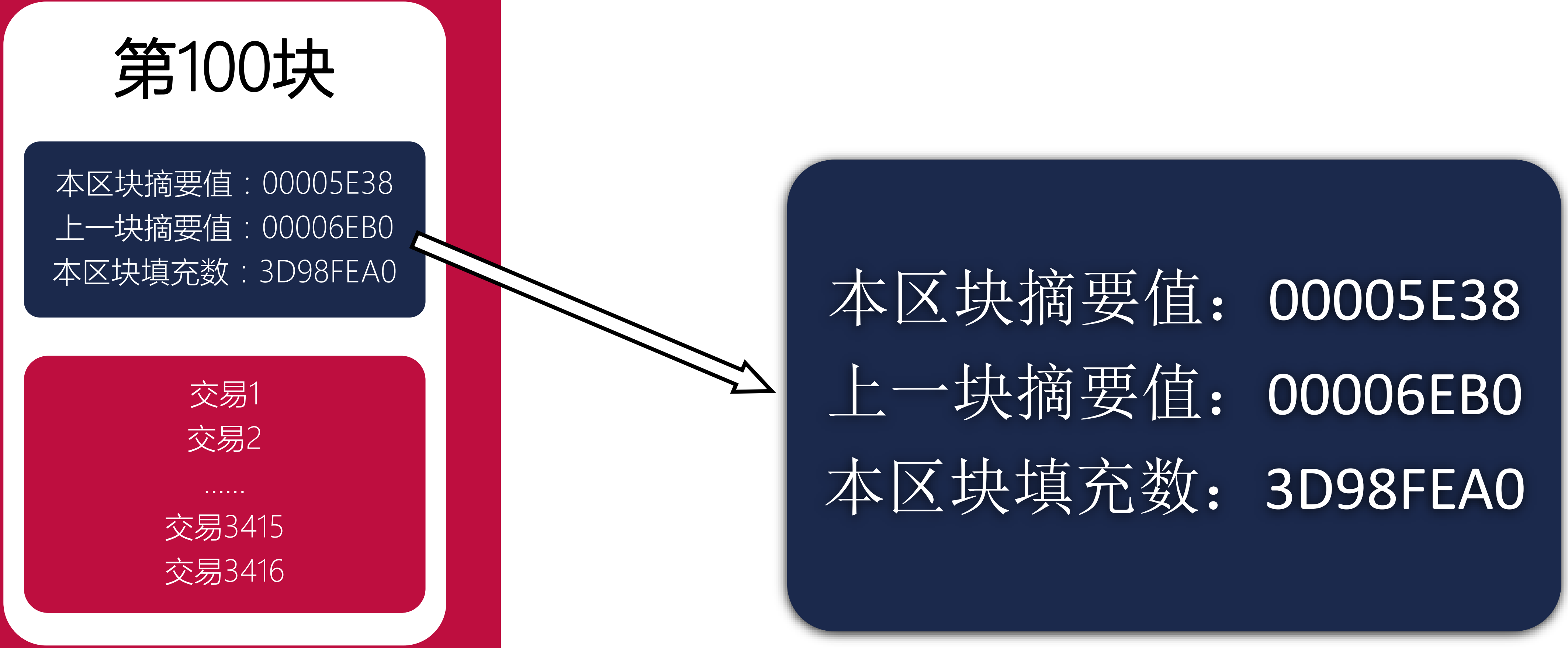
区块信息

本区块摘要值：00005E38
上一块摘要值：00006EB0
本区块填充数：3D98FEA0

交易信息

交易1
交易2
……
交易3415
交易3416

“区块”
是长这个样子的



第100块

本区块摘要值：00005E38
上一块摘要值：00006EB0
本区块填充数：3D98FEA0

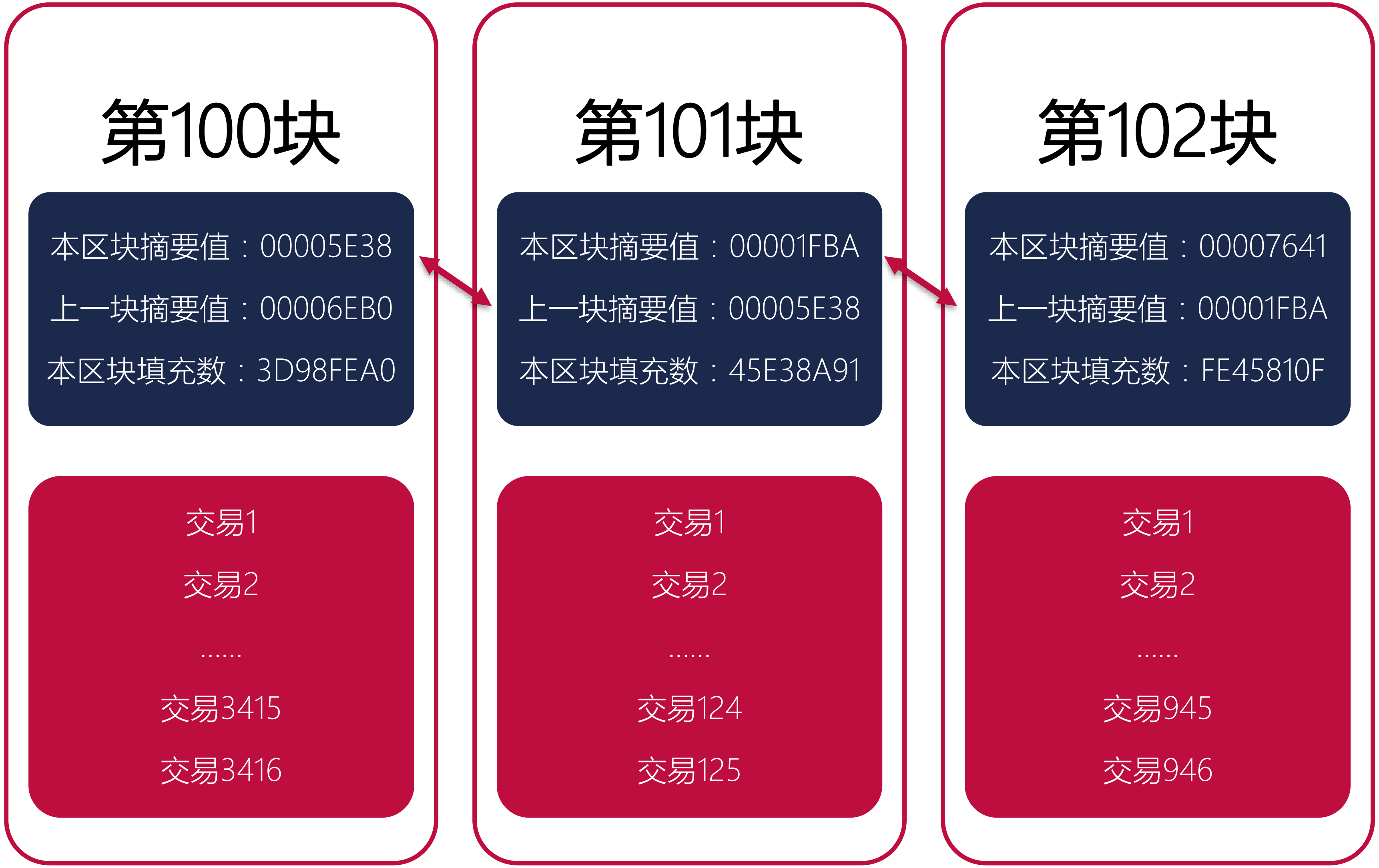
交易1
交易2
……
交易3415
交易3416

本区块摘要值：00005E38
上一块摘要值：00006EB0
本区块填充数：3D98FEA0

“区块”

连成

“链”



第100块

本区块摘要值：00005E38

上一块摘要值：00006EB0

本区块填充数：3D98FEA0

交易1

交易2

……

交易3415

交易3416

第101块

本区块摘要值：00001FBA

上一块摘要值：00005E38

本区块填充数：45E38A91

交易1

交易2

……

交易124

交易125

第102块

本区块摘要值：00007641

上一块摘要值：00001FBA

本区块填充数：FE45810F

交易1

交易2

……

交易945

交易946

Contents

2 区块链技术

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

区块链技术的4个基本性质

- 点对点对等网络
- 共识机制
- 数据可验证
- 奖励合作的制度设计

区块链技术的4个基本性质

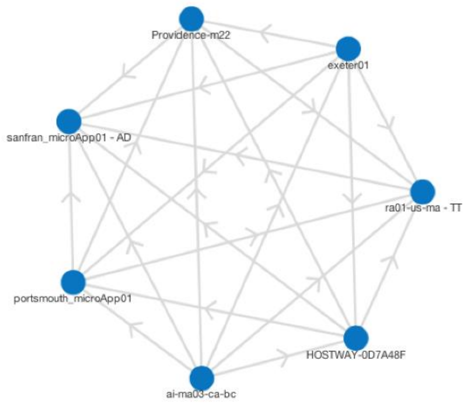
点对点对等网络

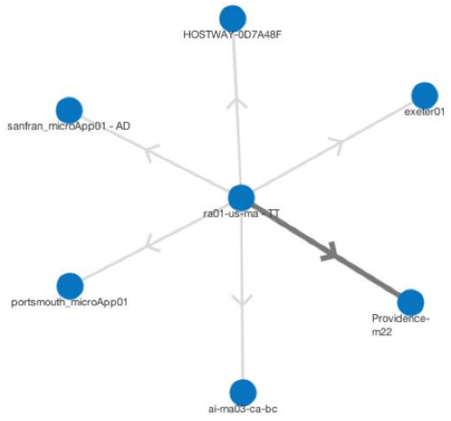
共识机制

数据可验证

奖励合作的制度设计

- ■ 网格网络（Mesh） vs 轴辐网络（Hub-and-Spoke）
- ■ 权限对等、数据公开 vs 中央服务器分配权限
- ■ 数据分布式、高冗余存储 vs 多点备份





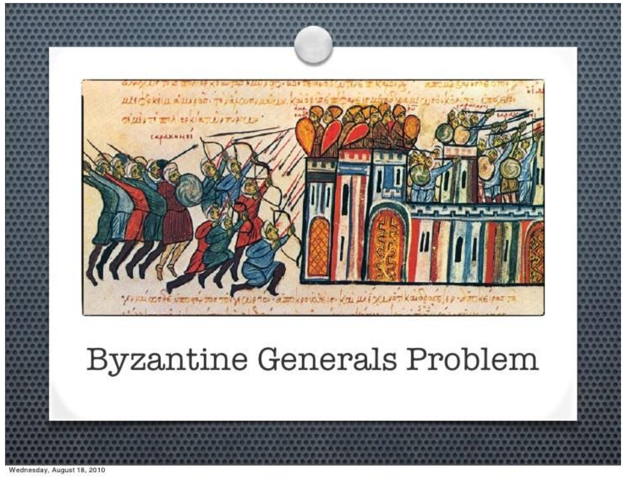
点对点对等网络

共识机制

数据可验证

奖励合作的制度设计

- 拜占庭将军问题
  - 工作量证明
  - 权益证明
  - 基于信任的Quorum



Byzantine Generals Problem

Wednesday, August 18, 2010

- 共识机制防止了“双重支付”
  - 信息复制的零边际成本 vs 价值的唯一不可复制性
  - 信息互联网 → 价值互联网

点对点对等网络

共识机制

数据可验证

奖励合作的制度设计

PKI公钥体系

- 数字签名提供密码学证据
- 零知识证明

不可变数据

- 只可添加，不可编辑
- 不可变数据 + 时间戳，为互联网加上了时间轴

点对点对等网络

共识机制

数据可验证

奖励合作的制度设计

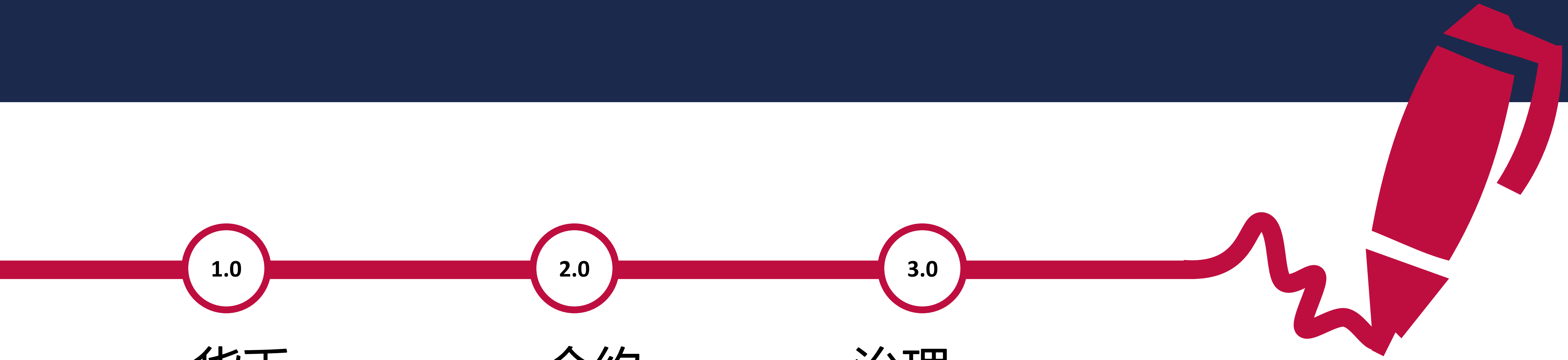
- 非合作博弈 —— 不基于信任，无外部强制力
- 合作是一种演化稳定策略，合作达到纳什均衡
- 51%攻击问题

Contents

3 区块链与未来

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

区块链技术发展的三个阶段（领域）



1.0

货币
Currency

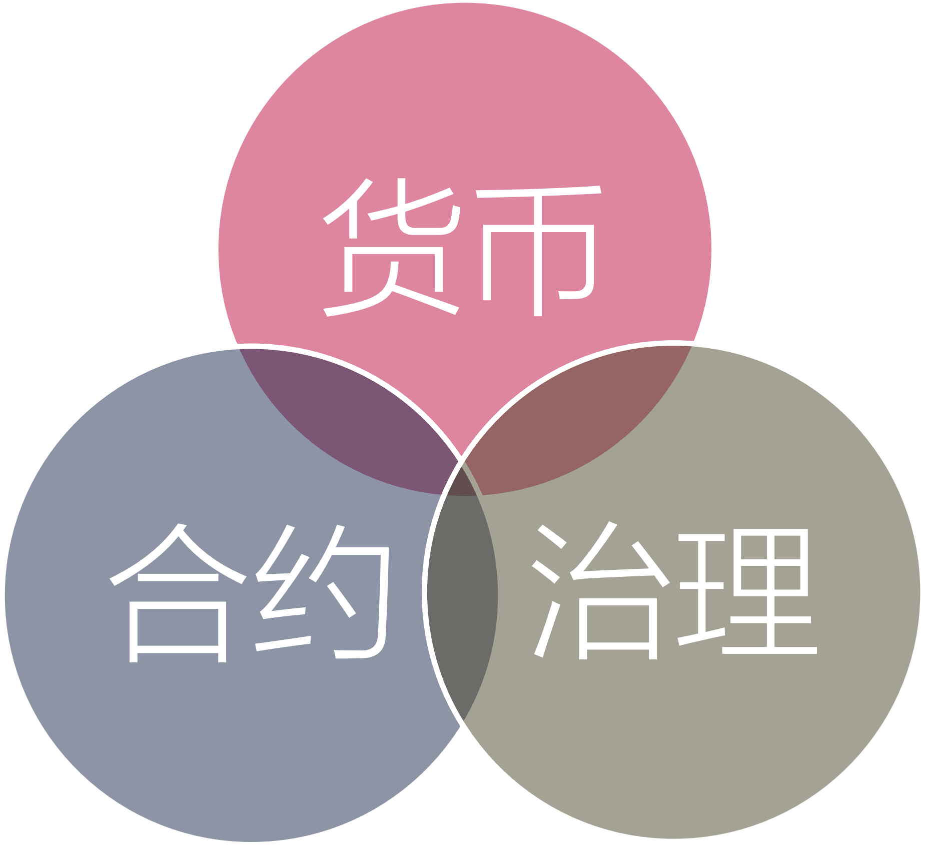
2.0

合约
Contract

3.0

治理
Governance

三个领域交叉重叠



货币

合约

治理

1.0

货币 Currency

- ■ 货币的发行机制
- ■ 货币的分配机制
- ■ 货币的币值调节机制

2.0

合约 Contract

- 股权、债权
- 证券与金融合约
- 互助保险
- 权利的登记、转让

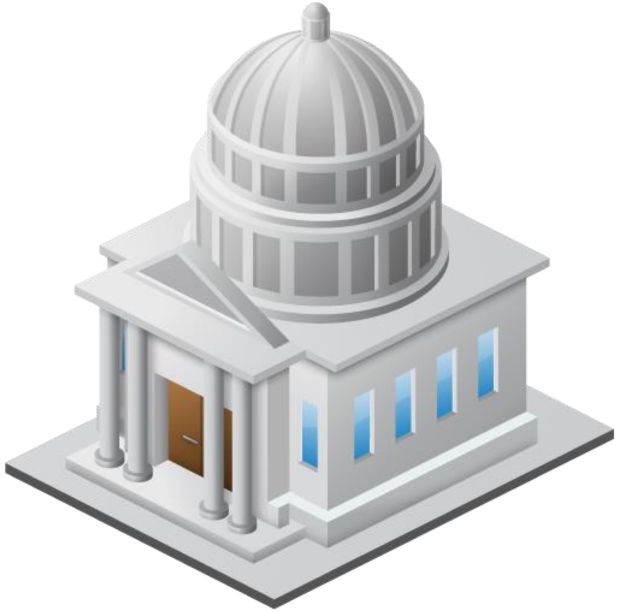
- 博彩
- 防伪
- 物联网
- 智能合约

3.0

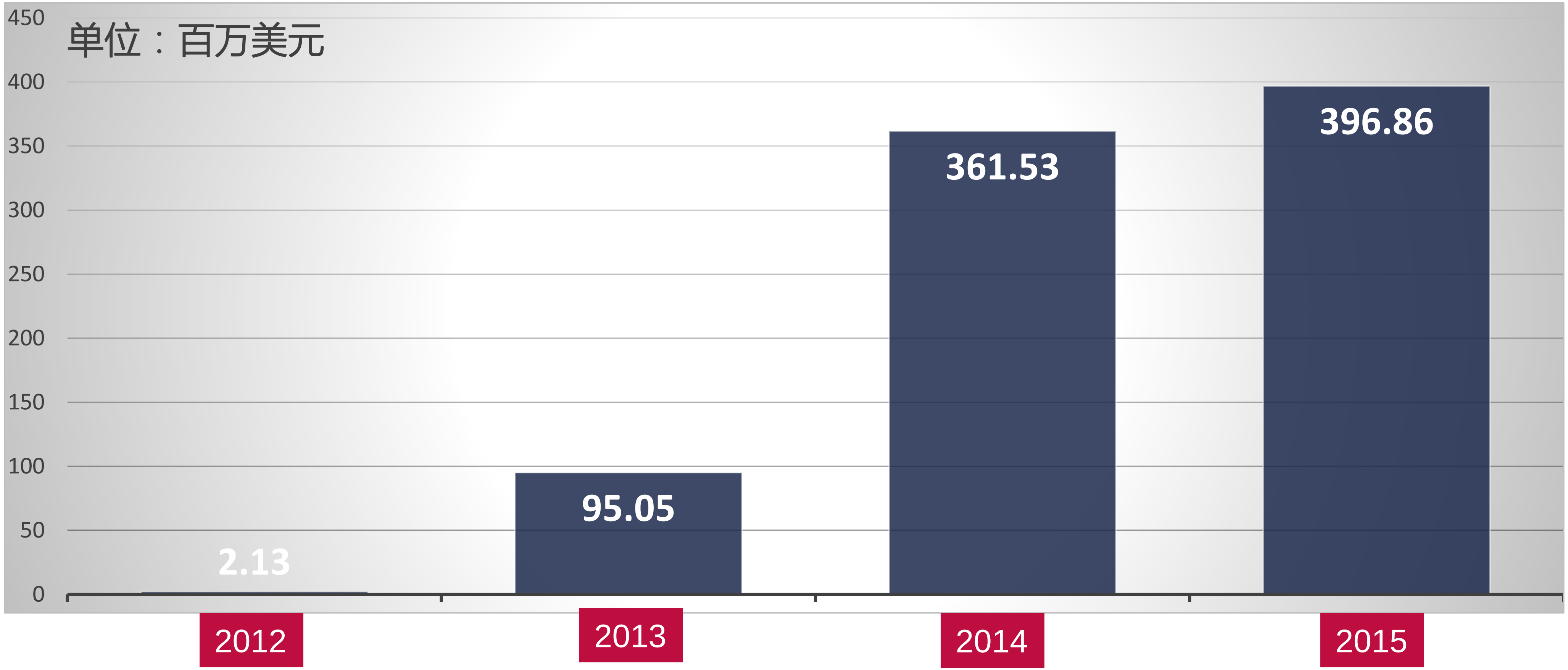
治理 Governance

- 身份认证
- 公证、见证
- 司法仲裁
- 投票

- 健康管理
- 人工智能
- 去中心化自治组织



区块链领域的风险投资趋势



Contents

Thank You

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks