区块链的前世今生

BLOCKCHAIN

分享人：michael.li

Blockchain


BTC/USDT 9723.39 +17.37% ≈68258.19CNY
高 9723.39 低 8269.99 24H量 108013
MA5:8447.75 MA10:9267.83 MA30:8824.23
19875.84
20210.26
15862.84
11515.42
9723.39
7168.00
Huobi Global
3155.00
2820.58
10-29
2018-04-01
2018-08-26
2019-01-27
2019-06-23
VOL:251.7K MA5:218.1K MA10:198.9K
548.6K
分时 1分钟 5分钟 15分钟 30分钟 1小时 4小时 1天 1周 1月

1.WHAT

2.WHY

3.HOW

4.CHANCE

1

What

什么是区块链?

区块链（Blockchain）结构首次为人关注，源于 2009 年初上线的比特币（Bitcoin）开源项目。从记账科技数千年的演化角度来看，区块链实际上是记账问题发展到分布式场景下的天然结果。

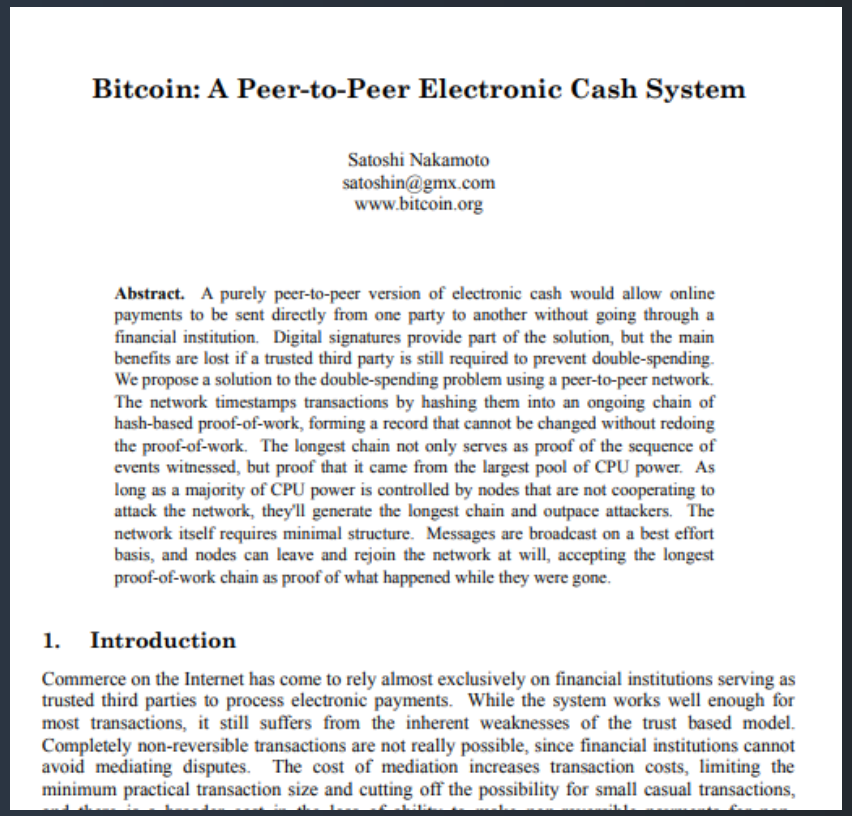
Wikipedia 上给出的定义中，将区块链类比为一种分布式数据库技术，通过维护数据块的链式结构，可以维持持续增长的、不可篡改的数据记录。

狭义上，区块链是一种以区块为基本单位的链式数据结构，区块中利用数字摘要对之前的交易历史进行校验，适合分布式记账场景下防篡改和可扩展性的需求。

广义上，区块链还指代基于区块链结构实现的分布式记账技术，包括分布式共识、隐私与安全保护、点对点通信技术、网络协议、智能合约等。

1

What



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,

+

什么是区块链

1

What

区块链的特点：

去中心化

去信任化

数据共享

不可篡改

什么是区块链

1

What

区块链的分类

公有链：以比特币、以太坊为代表的完全去中心化的应用

私有链：总公司和分公司，各部门之间数据共享。

联盟链：主要用于商业公司中的合作，所有节点不能随意进出，有准入控制，例子是超级账本。

什么是区块链

1

What

区块链的发展

区块链1.0 ： 比特币

区块链2.0 ： 以以太坊为代表的智能合约

区块链3.0 ： 超级账本、EOS

什么是区块链

2

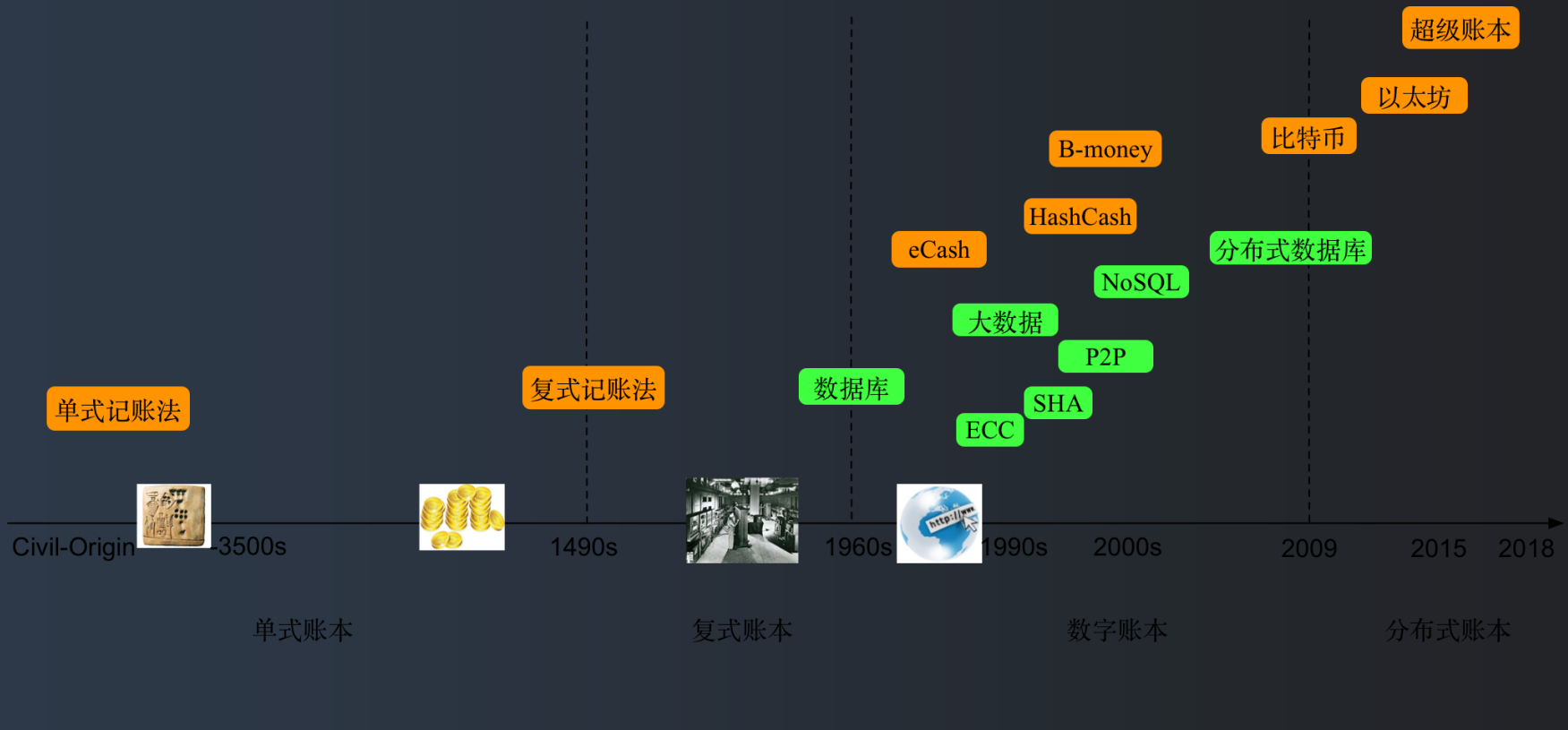
Why

为什么是区块链

阶段	时期	主要特点
阶段一：简单账本	约公元前 3500 年 ~ 15 世纪	使用原始的单式记账法（Single Entry Bookkeeping）
阶段二：复式账本	15 世纪 ~ 20 世纪中期	现代复式记账法（Double Entry Bookkeeping）出现和应用
阶段三：数字化账本	20 世纪中期 ~ 21 世纪初	物理媒介账本演化到数字化账本
阶段四：分布式账本	2009 年至今	区块链为代表的分布式账本相关思想和技术出现

2

Why



\+

为什么是区块链

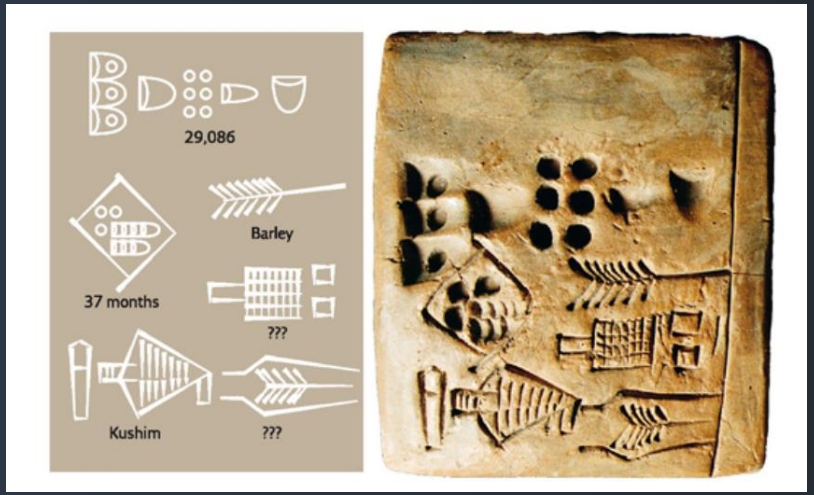
2

Why

阶段一：单式账本

人类文明早期，就已经产生了记账需求和相关活动。

已知最早的账本是“库辛（Kushim）泥板”，于 1929 年发掘于幼发拉底河下游右岸的伊拉克境内。据鉴定，库辛泥板属于公元前 3500 ~ 前 3000 年的乌鲁克城（Uruk，美索不达米亚西南部苏美尔人的古城），其内容据破译为“37 个月收到了 29086 单位的大麦，并由库辛签核”。如下图所示。



为什么是区块链

2

Why

阶段二：复式账本

复式记账法：前所未有的繁荣的商业活动催生了更先进的记账方式。复式记账法将单一中心记录分拆为多个科目，极大提高了账目的可靠性，一旦发现问题，方便追查根源。

复式记账法原理并不复杂。由于交易的本质是将某种价值从来源方转移到目标方，因此可将每笔交易分别在贷方（来源方）和借方（目标方）两个科目进行记录，且借贷双方的总额应该时刻保持相等（即守恒）。

复式记账法虽然解决了单个记账人所持本地账本可信的问题，但是仍然无法解决多方之间账本的可信互通问题。例如，投资者如何确保所投资企业的账目没有作假？贸易双方产生交易纠纷时该以谁的账本为准？这些问题的解决要等到数百年以后了。

为什么是区块链

2

Why

阶段三：数字化账本

如果要评价 20 世纪最伟大的十大发明，数字计算机一定会入围。它在物理世界之外开创了全新的赛博空间，为人类社会的方方面面都带来了巨大变化。早期计算机很重要的用途之一便是进行账目相关的统计处理。1951年，全世界首台商用计算机 UNIVAC，即为美国人口普查局所使用。

使用计算机，不但可以提高大规模记账的效率，还可以避免人工操作的错误。为了更好的管理统计数据，人们发明了专门的数据库技术。从最早的网状数据库（Network Databases）和层次数据库（Hierarchical Databases），到开创意义的关系型数据库（Relational Database），再到互联网出现后大量新需求催生的大数据、NoSQL 等技术，根源上都与记账问题息息相关。

在这一阶段，记账方法本身并没有太多创新，但由于数字媒介的出现，使得账本的规模、处理的速度、账本的复杂度，都有了天翻地覆的提升。而这些为后来包括电子商务、互联网金融在内的多种数字化服务奠定了技术基础。

为什么是区块链

2

How

基本原理：

区块链的基本原理理解起来并不复杂。首先来看三个基本概念：

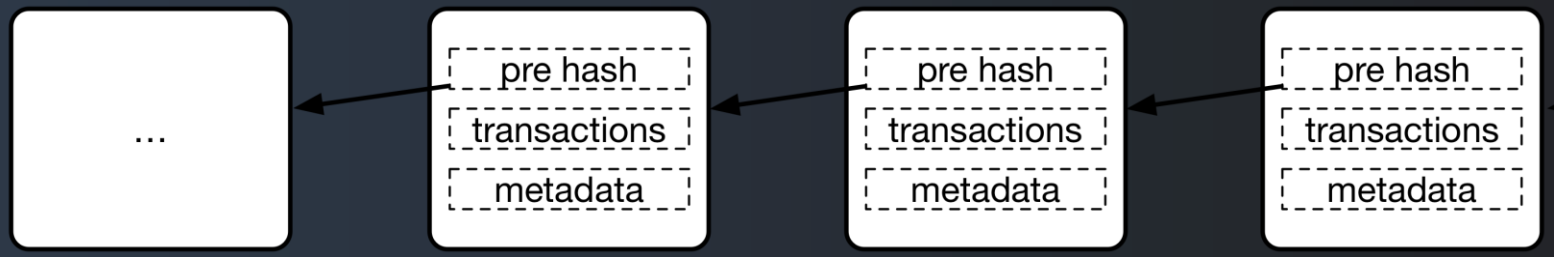
交易（Transaction）：一次对账本的操作，导致账本状态的一次改变，如添加一条转账记录；
区块（Block）：记录一段时间内发生的所有交易和状态结果等，是对当前账本状态的一次共识；
链（Chain）：由区块按照发生顺序串联而成，是整个账本状态变化的日志记录。
如果把区块链系统作为一个状态机，则每次交易意味着一次状态改变；生成的区块，就是参与者对其中交易导致状态改变结果的共识。

区块链的目标是实现一个分布的数据记录账本，这个账本只允许添加、不允许删除。账本底层的基本结构是一个线性的链表。链表由一个个“区块”串联组成（如下图所示），后继区块中记录前导区块的哈希（Hash）值。某个区块（以及块里的交易）是否合法，可通过计算哈希值的方式进行快速检验。网络中节点可以提议添加一个新的区块，但必须经过共识机制来对区块达成确认。

区块链是怎么实现的？

2

How



区块链是怎么实现的？

3

How

基本技术：

P2P 没有服务器和客户端，所有节点都是平等的。

密码学——哈希(HASH) 将不同长度的数据转换成固定长度的哈希值

MD5、SHA1、SHA2、（SHA2-256）

加解密算法
对称加密和非对称加密

共识算法
强一致性、最终一致性
Paxos、拜占庭算法

区块链是怎么实现的？

4

Chance

我们失去了什么机会?

挖矿

卖矿机—比特大陆

暴富—炒币

我们还有什么机会?

去信任（去中介）

价值转移

数据共享

我们有什么机会？

参考资料

《比特币白皮书—一种点对点的电子现金系统》

《区块链技术指南》 gitbook 杨宝华yeasy

我们有什么机会？

感谢大家的收看

T H A N K S

Thank you