区块链的技术原理与发展现状

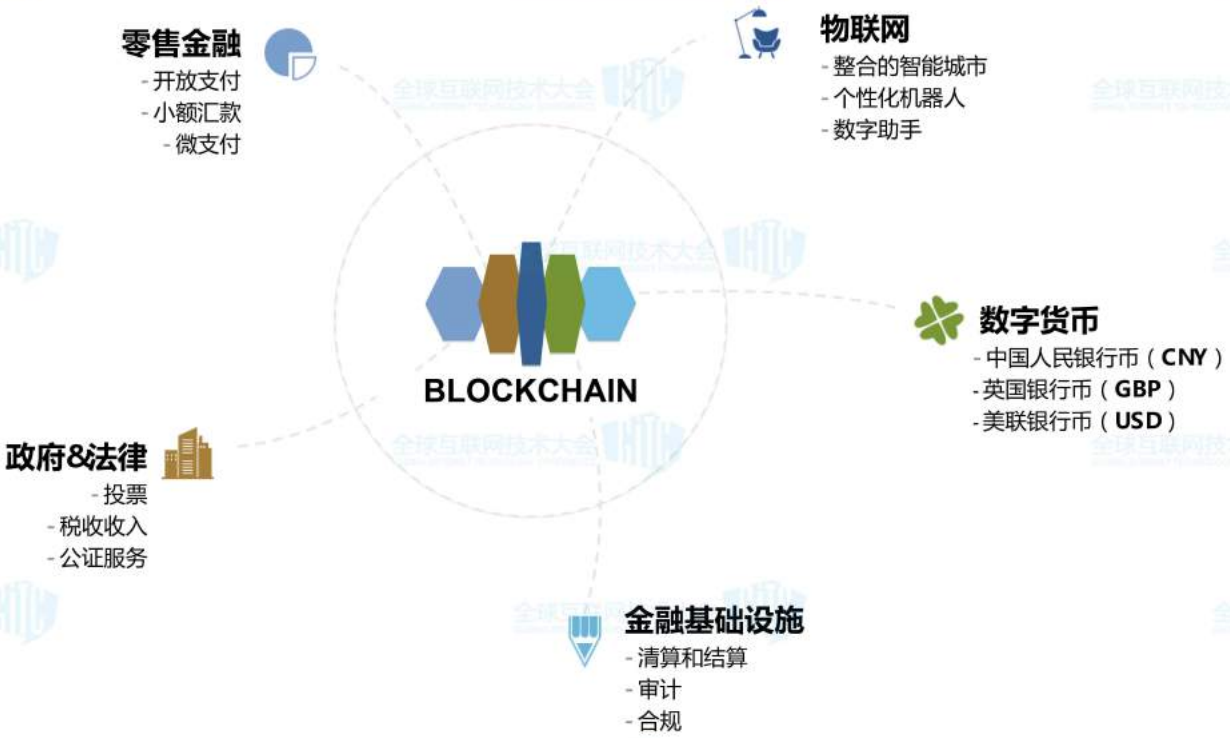
OKCoin币行&OKLink CTO 孙忠英

互联网是传输信息的网络　区块链是传输价值的网络

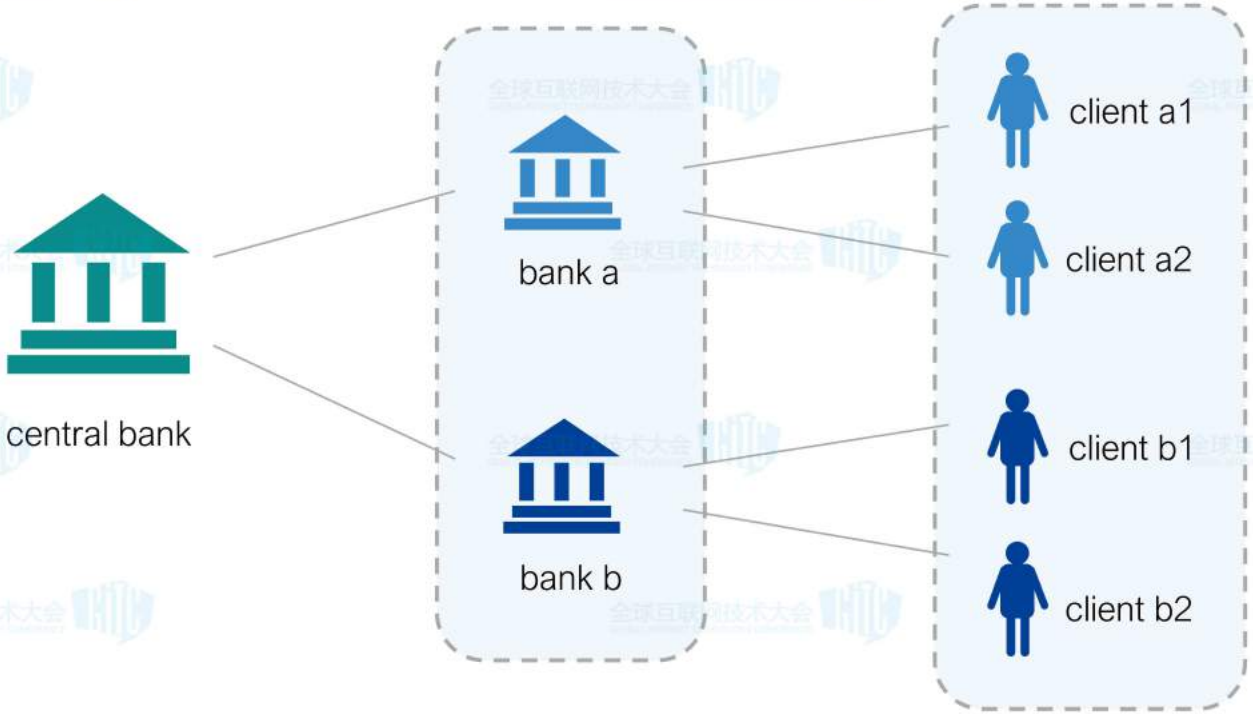
互联网与移动互联网

区块链技术

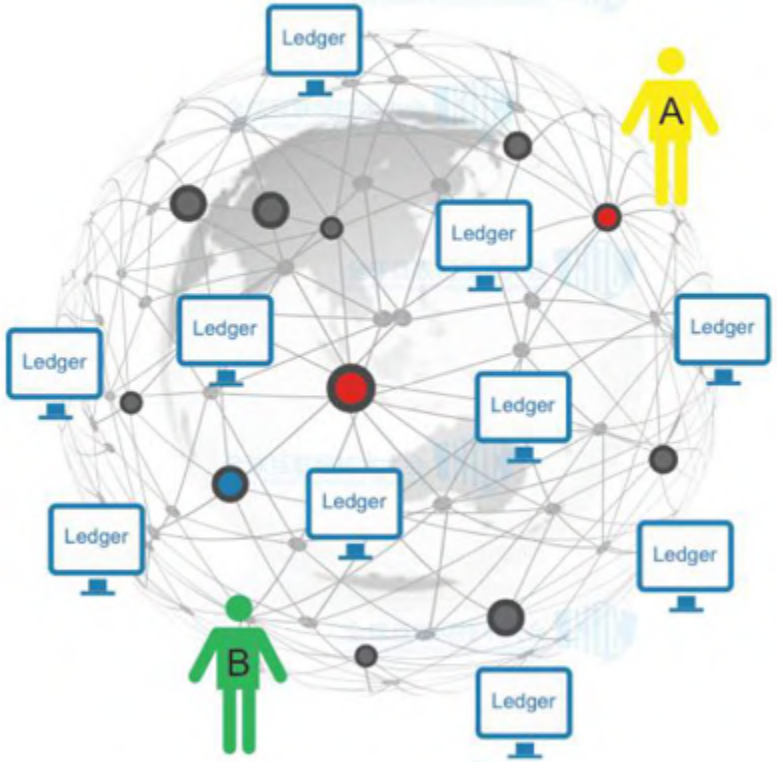
区块链巨大的应用空间


零售金融
- 开放支付
- 小额汇款
- 微支付
物联网
- 整合的智能城市
- 个性化机器人
- 数字助手
BLOCKCHAIN
数字货币
- 中国人民银行币（CNY）
- 英国银行币（GBP）
- 美联银行币（USD）
政府&法律
- 投票
- 税收收入
- 公证服务
金融基础设施
- 清算和结算
- 审计
- 合规

原本：中心化的世界


central bank
bank a
bank b
client a1
client a2
client b1
client b2

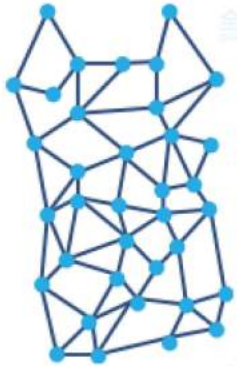
区块链：去中心化总账


Ledger
A
Ledger
Ledger
Ledger
Ledger
Ledger
Ledger
Ledger
Ledger
Ledger
B
Ledger

从中心化到去中心化的网络

集中式

分散式

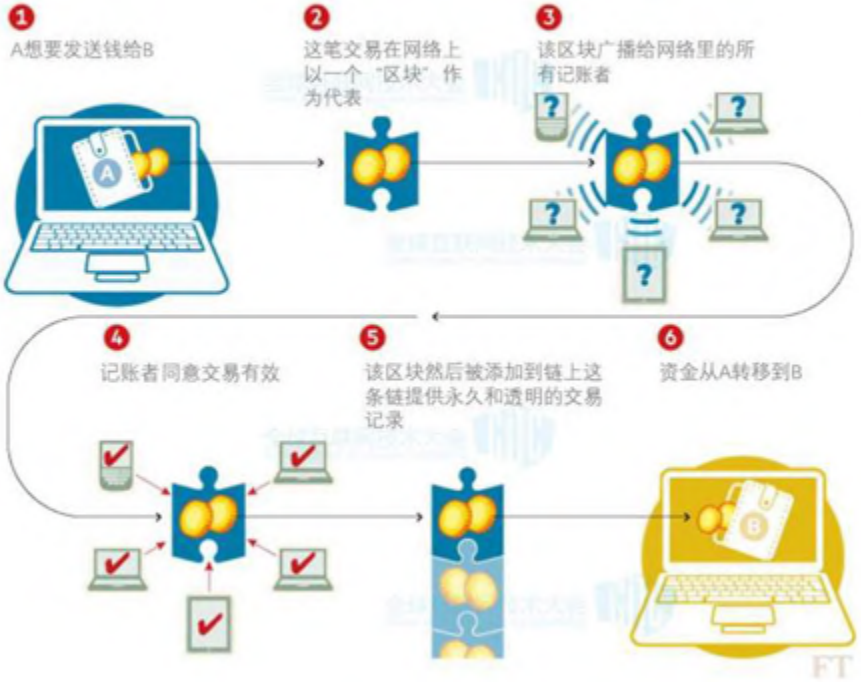


分布式

共享账本

- 记录商业网络中的所有交易
- 在参与者之间共享
- 参与者通过同步获取自己的备份
- 授权许可的，参与者只能看到适当的交易记录信息
- 共享的记录系统

划时代的点对点交易


1
A想要发送钱给B
2
这笔交易在网络上以一个“区块”作为代表
3
该区块广播给网络里的所有记账者
4
记账者同意交易有效
5
该区块然后被添加到链上这条链提供永久和透明的交易记录
6
资金从A转移到B
FT

区块链的技术基础

区块链源自比特币

区块链是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案

区块链的概念首次在2008年末由中本聪（Satoshi Nakamoto）发表在比特币论坛中的论文《Bitcoin: A Peer-to-Peer Electronic Cash System》提出。论文中区块链技术是构建比特币数据结构与交易信息加密传输的基础技术，该技术实现了比特币的挖矿与交易。中本聪认为：第一，借助第三方机构来处理信息的模式拥有点与点之间缺乏信任的内生弱点，商家为了提防自己的客户，会向客户索取完全不必要的信息，但仍然不能避免一定的欺诈行为；第二，中介机构的存在，增加了交易成本，限制了实际可行的最小交易规模；第三，数字签名本身能够解决电子货币身份问题，如果还需要第三方支持才能防止双重消费，则系统将失去价值。基于以上三点现存的问题，中本聪在区块链技术的基础上，创建了比特币。

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.

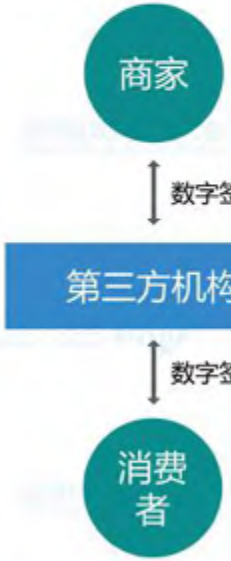
1. Introduction

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.

比特币与传统支付技术的区别

传统支付系统



记录账本

1.信用靠第三方维持，商家与消费者间缺少信任，需要获取客户不必要的信息。与现实中的消费不同。

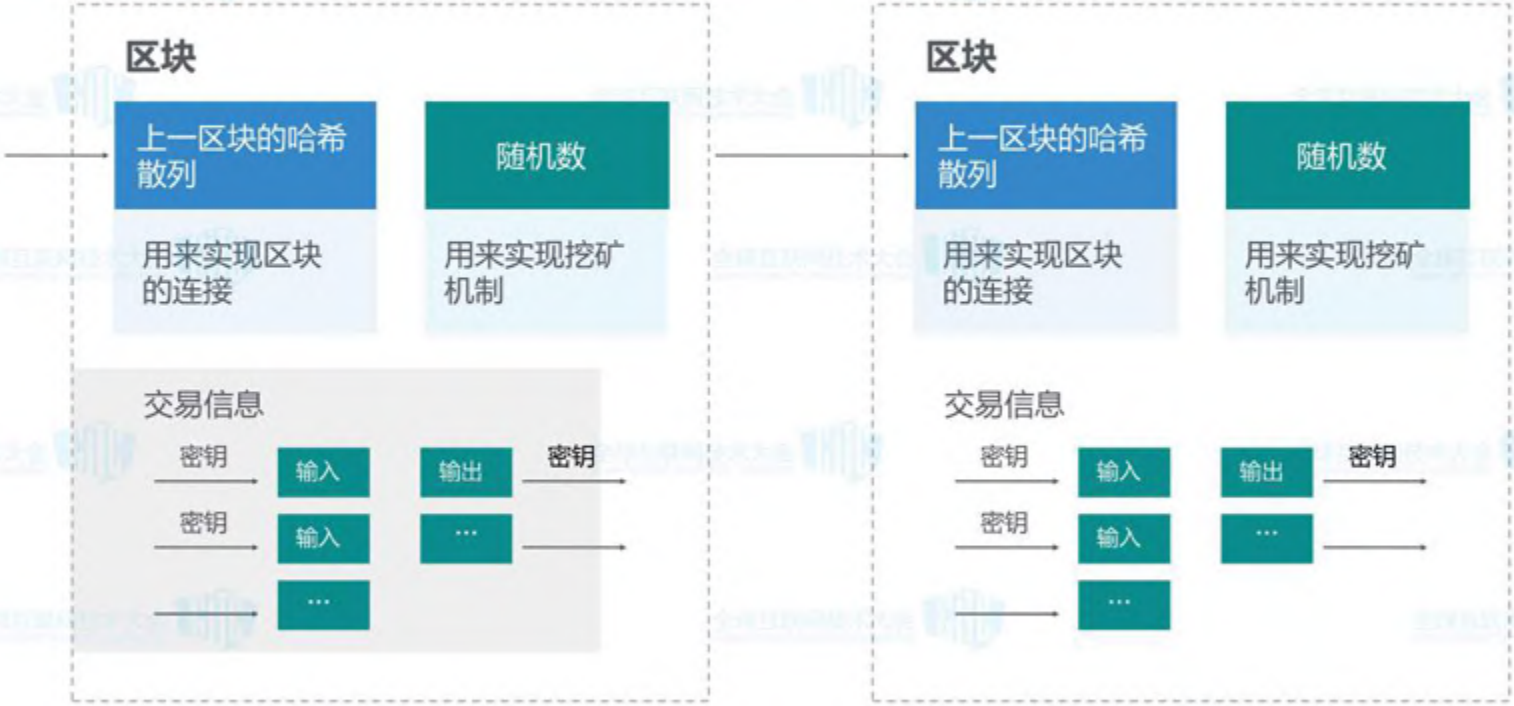
2.中介机构的存在，增加了交易成本，限制了最小交易规模。

3.使用了数字签名，却依然利用第三方防止双重消费。

区块链支付系统

这些优点的叠加可以解决两个长期存在于加密数字货币行业的问题：**“双花”问题和“拜占庭”将军问题。**

区块和区块链的组成


区块
上一区块的哈希散列
随机数
用来实现区块的连接
用来实现挖矿机制
交易信息
密钥
输入
密钥
输入
...
输出
密钥
...
区块
上一区块的哈希散列
随机数
用来实现区块的连接
用来实现挖矿机制
交易信息
密钥
输入
密钥
输入
...
输出
密钥
...

共识问题拜占庭将军问题

共识机制

- POW
- POS
- DPOS
- PBFT

智能合约

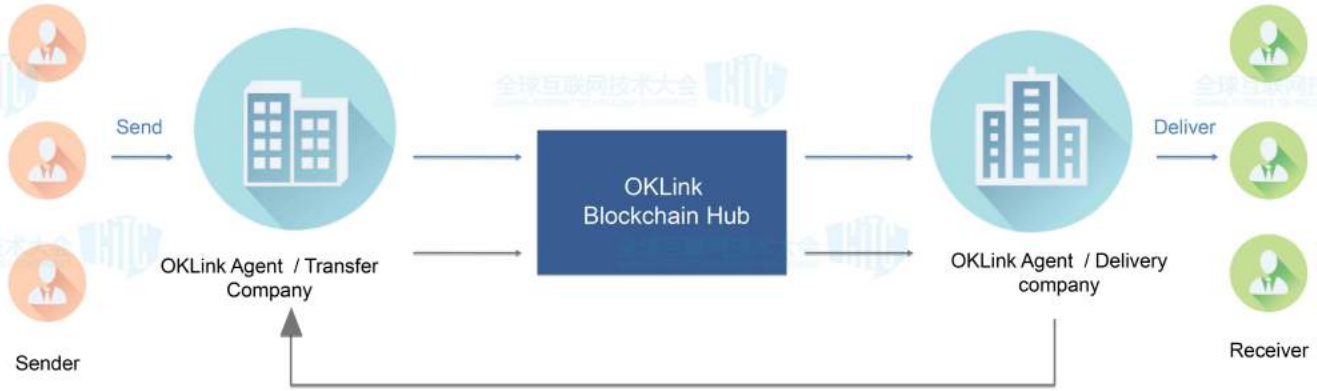
- 合约中的商业规则内嵌在区块链系统中，在交易时被执行
- 可验证的 / 被签署的
- 编码在编程语言中
- 案例：

  在公司债权发生转移时执行定义的合同条款

区块链的分类：公有链、私有链、联盟链

区块链落地应用

区块链应用OKLink汇款流程图



OKLink已加入的重点合作伙伴

THANKS