ThoughtWorks®

TiD 2017

解析区块链

讲师介绍

刘尚奇，ThoughtWorks中国区区块链能力负责人，信息安全专业，为多家大型企业提供架构设计与服务化转型工作，熟悉区块链技术、微服务架构、分布式系统、持续交付等领域。

AGENDA

1. 互联网上的价值转移
2. 什么是区块链
3. 区块链的应用
4. 区块链的历史与发展
5. 区块链的未来

ThoughtWorks®

互联网上的价值转移

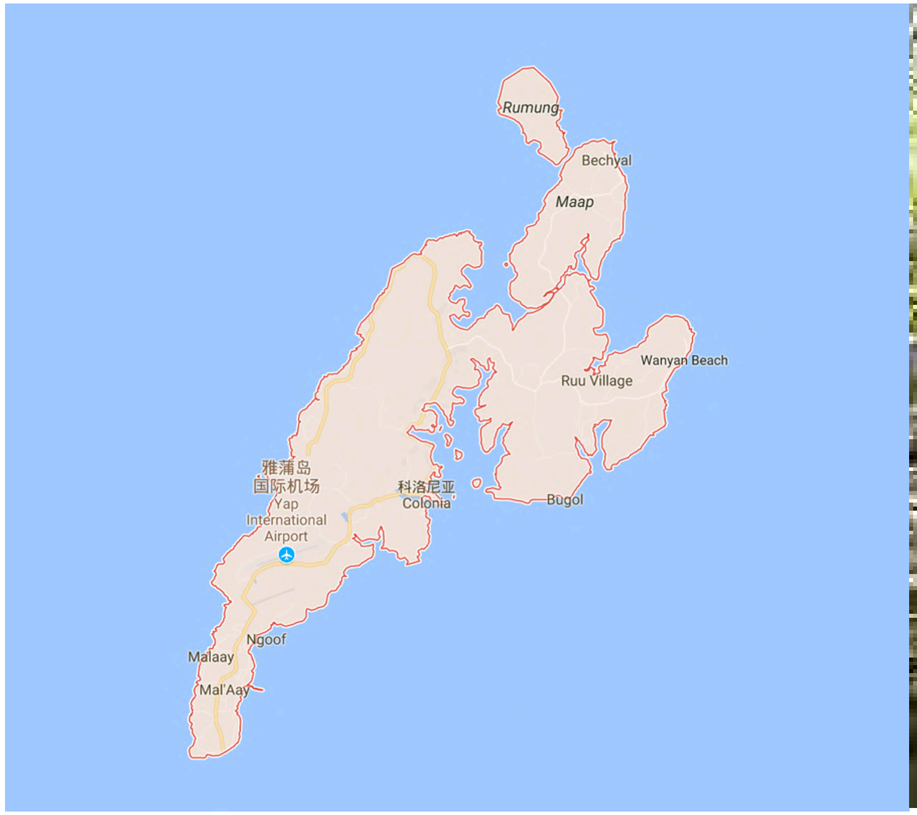
Money on the Internet

如何在网络中以每个人都认可的方式，将某一部分价值精确地从某个地址转移到另一个地址

互联网上的价值转移

- 互联网是为信息传输而设计，而不是价值转移
- 传统的货币不是为互联网设计的，在互联网上面临**交易欺诈**的风险
  - 所有权
  - 双重支付
- 如果在互联网上没有央行或**中央机构**，我们怎么知道每个人**持有多少价值**?

雅浦岛上的价值转移



雅浦岛与巨石币

雅浦岛上的价值转移

沉没的巨石币

基于集体共识的价值转移

- 基于公开声明的所有权
- 基于集体共识验证的交易
- 历史不可篡改的账簿

建立信用共识为基础的价值转移

- 能够证明每个人持有的价值(所有权)
- 具备去信任机制的交易验证(不需要相信环节中的任何人和机构)
- 交易历史不可篡改
- 自动运行
- 不需要第三方中介

人类跨越国家、种族、宗教、政治、文化...少数能获得共识的事物之一：数学

ThoughtWorks®

什么是区块链

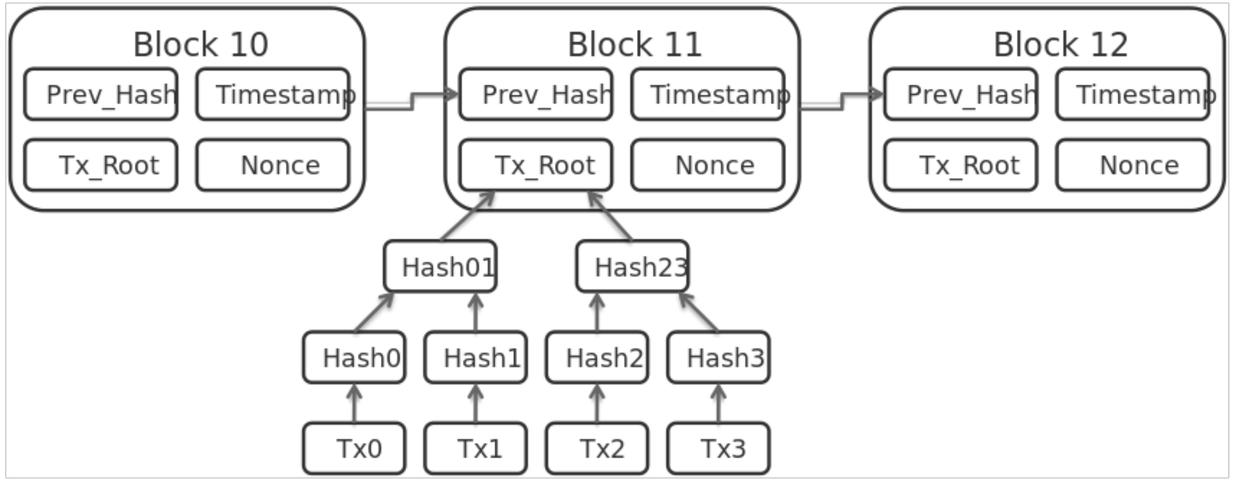
What is blockchain

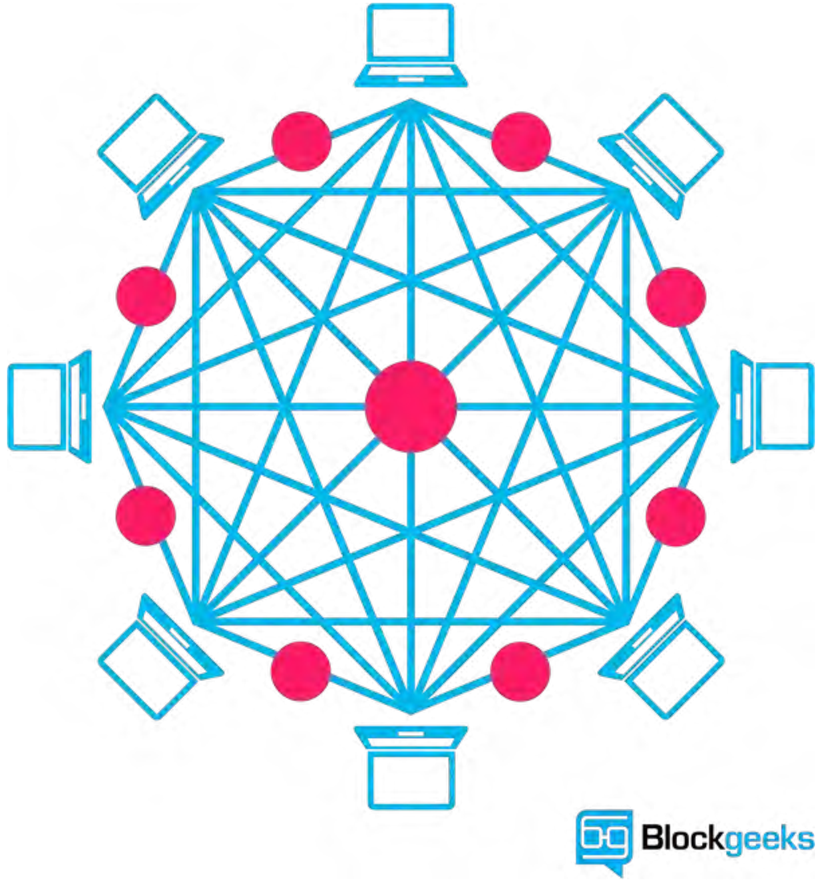
什么是区块链

"The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value."

Don & Alex Tapscott, authors Blockchain Revolution (2016)

什么是区块链


Block 10
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 11
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 12
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3


Blockgeeks

什么是区块链

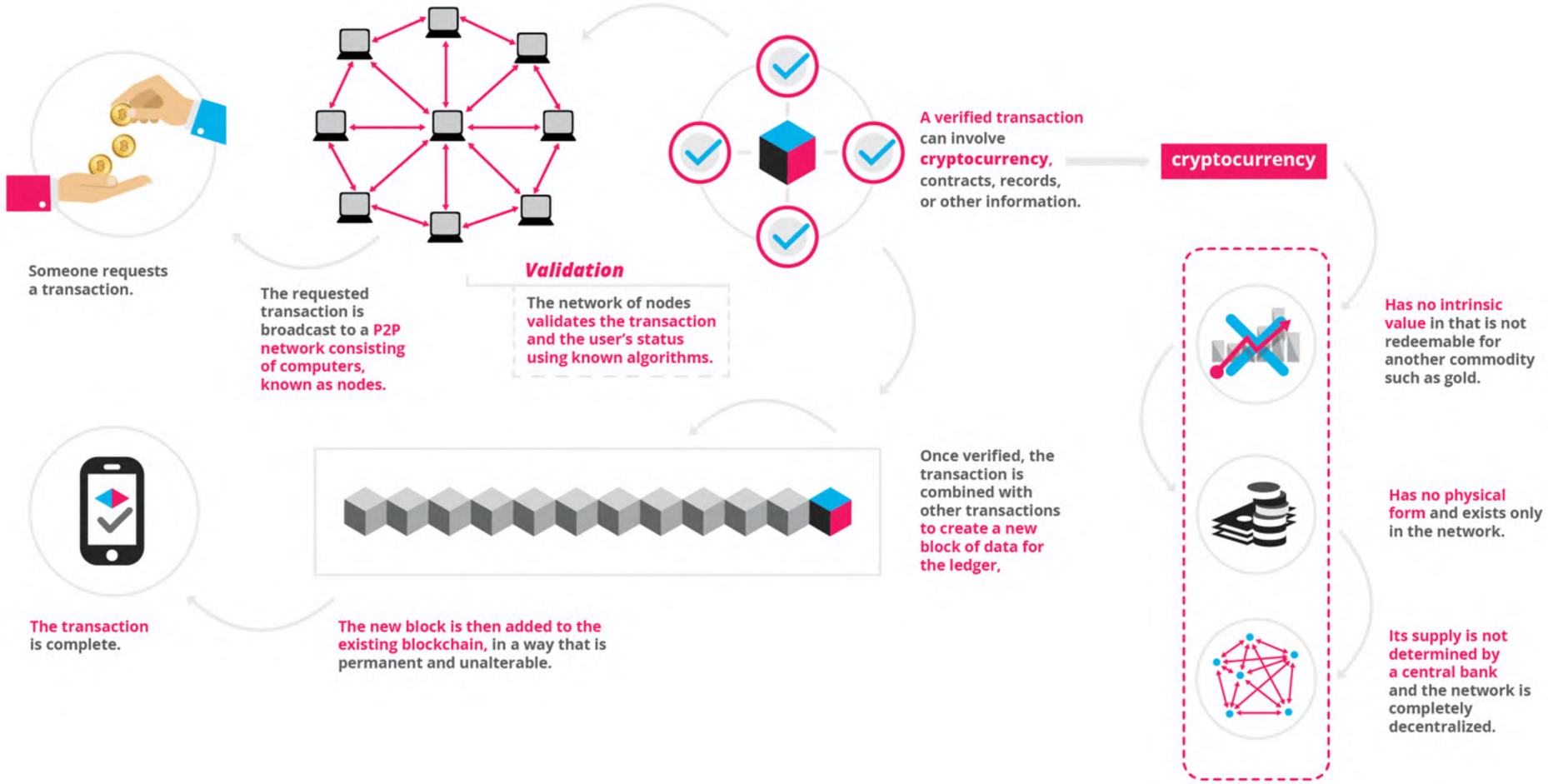
可以把区块链看做某种形式的数据存储

- 通常包含的是金融交易
- 在多个系统间**近实时(real-time)**地复制
- 通常构建在**对等网络(P2P Network)**上
- 通过**密码学**和**数字签名**机制保证身份、可靠性，确保数据写入读取权限
- 被设计为**难以改变的历史记录**，或者至少有人试图修改时可以很容易发现

区块链如何解决价值转移的挑战

- 证明每个人持有的价值(所有权)?
  - **公钥基础设置**(PKI)和**数字签名**
- 如何防止交易的欺诈与篡改?
  - 每笔交易都经过所有节点进行**独立验证**
  - 由**默克尔树(Merkle Tree)**和**哈希区块链**构成的不可篡改的历史记录
- 需要中央银行为信任背书?
  - **共享**的账本
  - 每个区块链节点都有**全量的数据**
  - 对记录的更新需要全部参与者达成**共识(Distributed Consensus)**

区块链如何运作



https://blockgeeks.com/guides/what-is-blockchain-technology/

ThoughtWorks®

区块链的应用

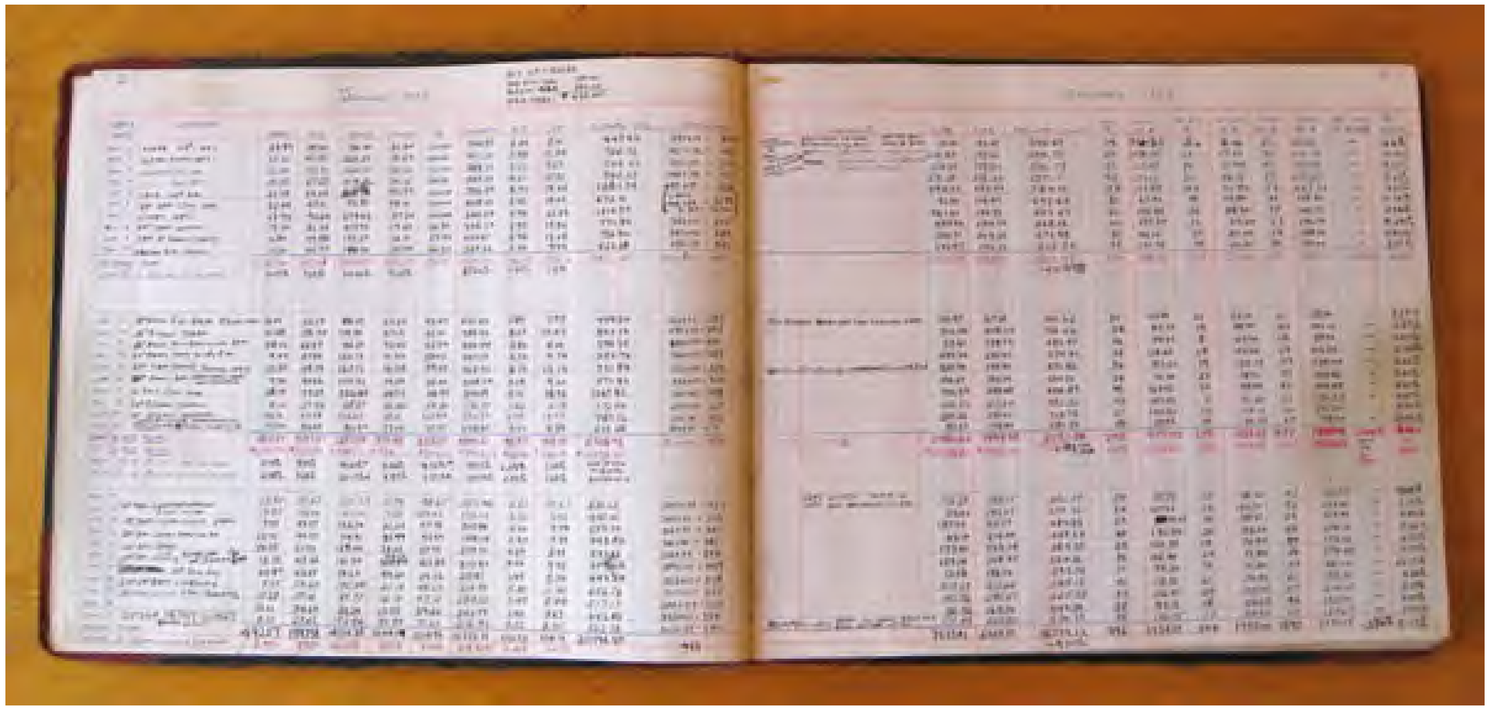
Use case of blockchain

区块链能力的核心价值

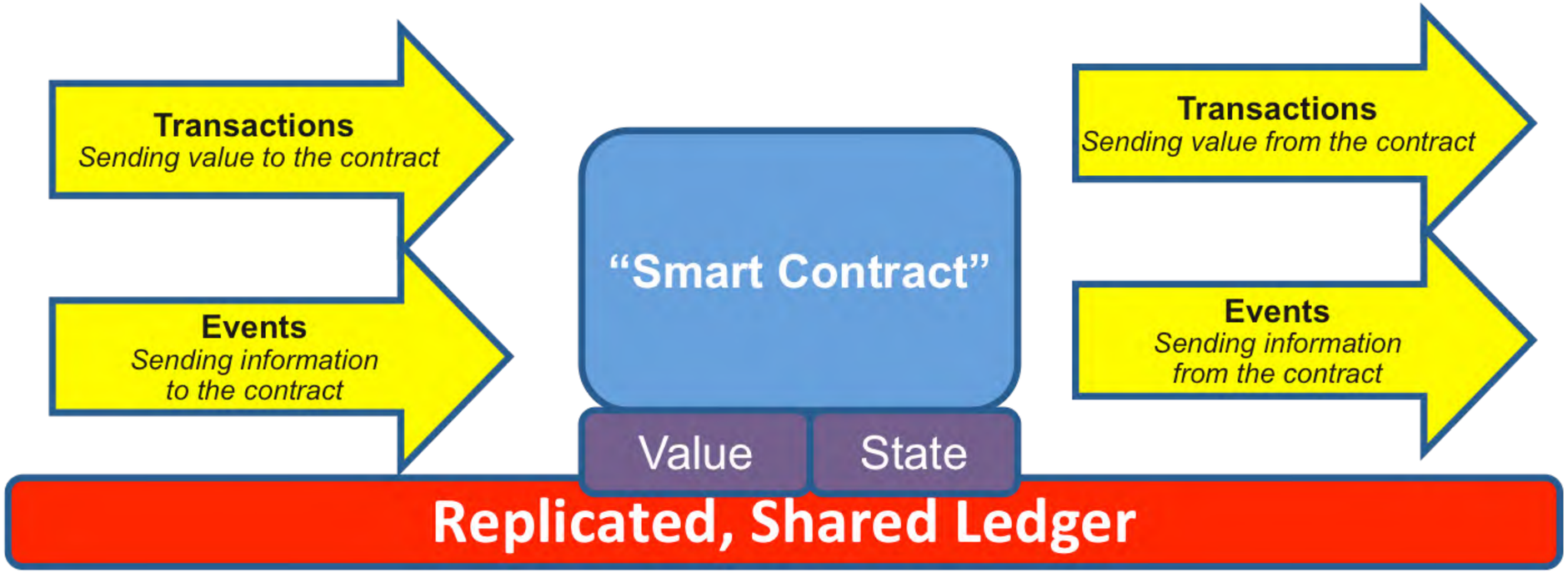

The Economist
OCTOBER 31ST–NOVEMBER 6TH 2015
Economist.com
Our guide to America's best colleges
Myanmar's free-ish election
Those ever-creative accountants
America takes the fight to IS
Coywolves: the new superpredator
The trust machine
How the technology behind bitcoin could change the world
IN BLOCKCHAIN WE TRUST

数字货币

不可篡改账本



智能合约



"一个智能合约是一套以数字形式定义的承诺（promises），包括合约参与方可以在上面执行这些承诺的协议。"

--尼克·萨博(Nick Szabo), 1995

智能合约

Traditional contracts	Smart contracts
1-3 Days	Minutes
Manual remittance	Automatic remittance
Escrow necessary	Escrow may not be necessary
Expensive	Fraction of the cost
Physical presence (wet signature)	Virtual presence (digital signature)

智能合约

```
pragma solidity ^0.4.11;

contract Purchase {
    uint public value;
    address public seller;
    address public buyer;
    enum State { Created, Locked, Inactive }
    State public state;

    function Purchase() payable {
        seller = msg.sender;
        value = msg.value / 2;
        require((2 * value) == msg.value);
    }

    ...

    /// 终止支付重新声明以太币，只能由卖家在合约锁定前调用
    function abort() onlySeller inState(State.Created)
    {
        Aborted();
        state = State.Inactive;
        seller.transfer(this.balance);
    }

    /// 买家确认支付。交易中必须包含2倍价格的以太币，这笔钱会被锁定在合约中，直到确认收货被调用。
    function confirmPurchase() inState(State.Created) condition(msg.value == (2 * value)) payable
    {
        PurchaseConfirmed();
        buyer = msg.sender;
        state = State.Locked;
    }

    /// 买家确认收货。这会释放锁定的以太币。
    function confirmReceived() onlyBuyer inState(State.Locked)
    {
        ItemReceived();
        state = State.Inactive;

        // 备注：实际可以同时由买家和卖家锁定保证金
        buyer.transfer(value);
        seller.transfer(this.balance);
    }
}
```

ICO(INITIAL COIN OFFERING)

ICO改编自证券界的Initial Public Offering(首次公开发行), 几个有代表性的国际ICO案例:

- 2013年7月,Mastercoin(现更名为Omni):可查的最早ICO项目,通过meta-protocol拓展比特币功能,募集5000 BTC。
- 2013年12月,NXT(未来币):首个完整的PoS区块链,曾经神秘的开发者,持续发展的强大社区。ICO神话:募集21 BTC(是的你没看错,21BTC,约等于当时6000美元),市值峰值曾到达过1亿美元。
- 2013年-2014年,Bitshares(比特股):曾经的“数字资产二代币三剑客”之一(另外两个为NXT和CounterParty),国内 数字货币界口水之源,毁誉参半。其社区培养了国内大量早期ICO以及数字资产爱好者。
- 2014年7月,Ethereum(以太坊):ICO时募集3万余个比特币曾创下纪录。将智能合约理念推进到极致的区块链项目 ,让全世界重新认识区块链公 有链的项目。近两年最成功的ICO,也是至今为止除比特币以外市值最高的数字货币/ 区块链项目。近期由于TheDAO事件影响晴雨不定。
- 2015年3月,Factom(公正通):双代币设计,首提存在性证明的区块链商业化以及由此导出的基金会与公司双机构设置。
- 2016年3月,Lisk:以太坊挑战者,利用侧链的Dapp解决方案。
- 2016年5月,TheDAO:等值1.5亿美元破世界纪录的ICO众筹,非典型ICO(其本身不是区块链)。向世界大声宣告智能合约时代到来后一个月即被黑客攻克,在历史上刻下了深深的双重惊叹号。

支付

解决问题

- 金融机构(特别是跨境机构)间对账、清算、结算成本高
- 很多手工操作，效率低
- 通过中介支付业务费用高昂

区块链思路

- 通过共享账本降低清算、结算成本
- 通过智能合约提高结算效率，优化账期
- 通过数字货币优化小额支付、跨境支付

资产注册

解决问题

- 股权、债券、票据等不同资产由不同机构托管
- 资产间交易成本高
- 凭证容易被伪造

区块链思路：

- 将各类资产整合到区块链上成为数字资产
- 无需中介就可以进行交易
- 凭证难以伪造，提高资产安全性

供应链

解决问题

- 信息不透明、不流畅，影响供应链的效率
- 供应链各主体间出现纠 纷时，举证和追责均耗时费力

区块链思路：

- 利用数字签名技术，可明确各环节职责
- 利用不可篡改的机制，可以对货物、商品进行防伪、溯源

everledger

公证

解决问题

- 存在性证明
- 完整性证明
- 所有权证明

区块链思路：

- 利用数字签名等密码学技术可以进行存在性证明、完整性证明、所有权证明的验证
- 通过透明的分布式账本，建立公证效力

身份管理/识别

解决问题

- 现在用户身份信息散落在各平台中，缺乏自动识别消费者身份的机制
- 传统金融体系中，不同机构间的用户身份信息和交易记录无法实现一致、高效的跟踪，使得监管机构的工作难以落到实处
- 消费者的身份和其他信息托管不周易导致隐私泄露

blockstack

区块链思路：

- 区块链通过共享的记录可以拉通用户的身份信息和交易记录，建立低成本的合规KYC
- 消费者只需提供签名就可以进行交易，减少信息泄露风险
- 用户可以通过将交易加密到只有给予秘钥检查的人才能访问，减少隐私泄露

共享经济

UBER

airbnb

去中介化

- 投票
- 互助保险
- 电子商务
- ....

AGORA VOTING

众托帮 ZHONGTOPIA 健康互助 普惠万家

OpenBazaar

ThoughtWorks®

区块链的历史与发展

History and evolution of blockchain

密码朋克

A Cypherpunk's Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of their interaction. Each party can speak about their own memory of this; how could anyone prevent it? One could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can speak to all the others and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient. When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must *always* reveal myself.

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.

Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. Furthermore, to reveal one's identity with assurance when the default is anonymity requires the cryptographic signature.

We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak. To try to prevent their speech is to fight against the realities of information. Information does not just want to be free, it longs to be free. Information expands to fill the available storage space. Information is Rumor's younger, stronger cousin; Information is fleeter of foot, has more eyes, knows more, and understands less than Rumor.

We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.

Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence. Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.

For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one's fellows in society. We the Cypherpunks seek your questions and your concerns and hope we may engage you so that we do not deceive ourselves. We will not, however, be moved out of our course because some may disagree with our goals.

The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace.

Onward.

Eric Hughes <hughes@soda.berkeley.edu>

9 March 1993

https://www.activism.net/cypherpunk/manifesto.html

比特币

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

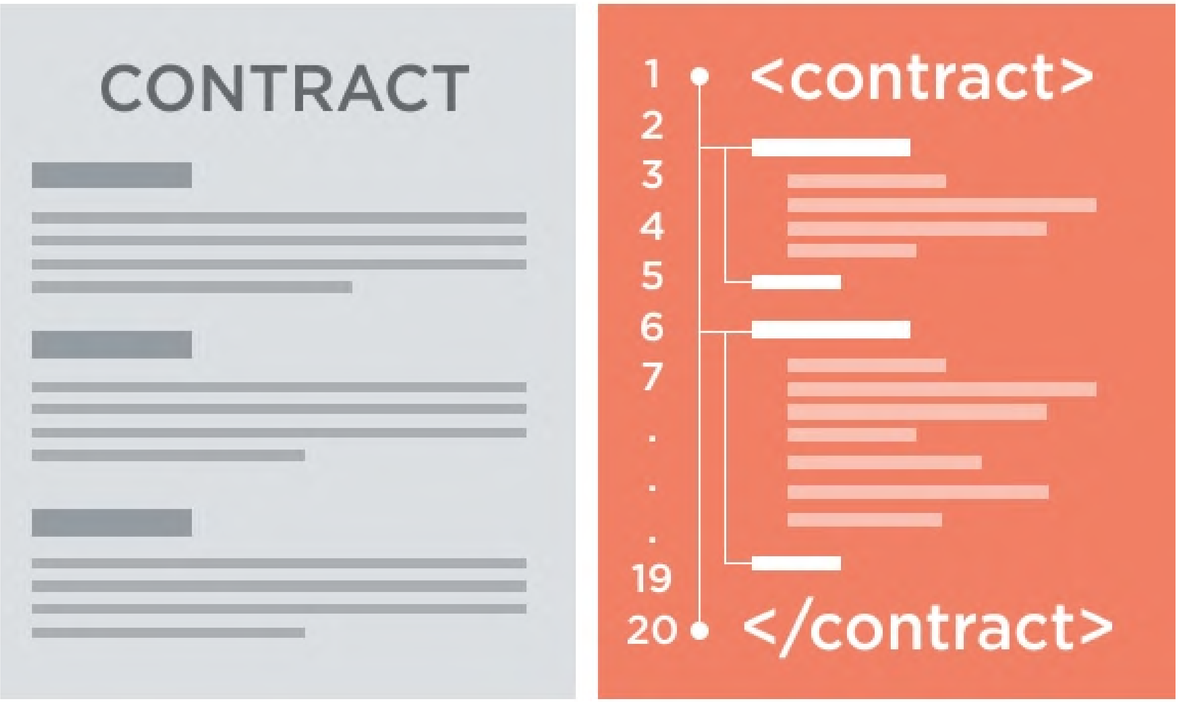
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

https://bitcoin.org/bitcoin.pdf

区块链


digital
exchange
business
data
bitcoin
digital
data
cash
virtual
exchange
electronic
currency
virtual
bitcoin
financial
cryptocurrency
protocol
coin
internet
smart
cash
ledger
crypto
market
market
Blockchain
money
concept
technology
technology
business
coin
finance
transaction
electronic
money
concept
transaction
contract
internet
currency
litecoin
node
Blockchain
financial
transaction
cryptocurrency
virtual

智能合约

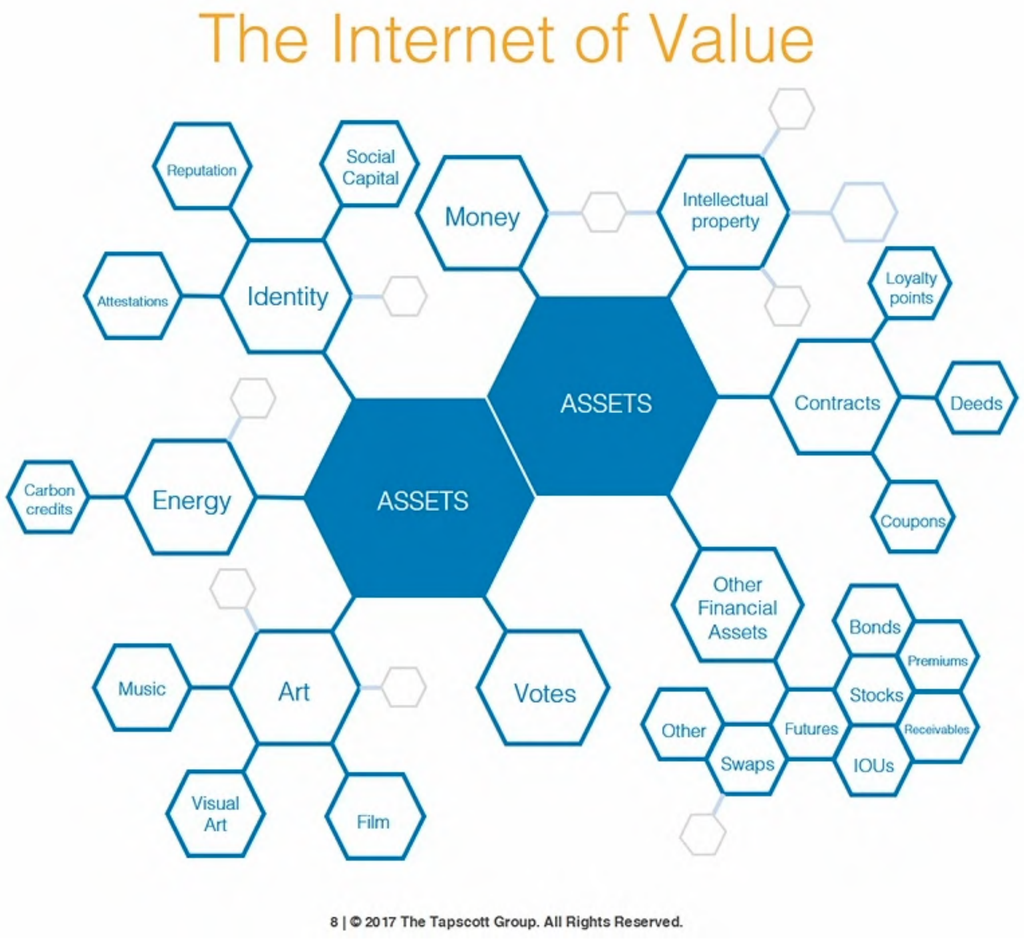


ThoughtWorks®

区块链的未来

Future of blockchain

价值互联网(INTERNET OF VALUE)



价值互联网(INTERNET OF VALUE)

- 信息互联网(Internet of Information)
  - TCP/IP = 通信协议
  - 革命性地改变了信息交换的方式
  - 杀手级应用： Email, Web

- 价值互联网(Internet of Value)
  - Blockchain = 价值转移协议
  - 建立起分布式的信任共识机制
  - 杀手级应用: Bitcoin

THANK YOU

For questions or suggestions:

Liu Shangqi
sqliu@thoughtworks.com

ThoughtWorks®