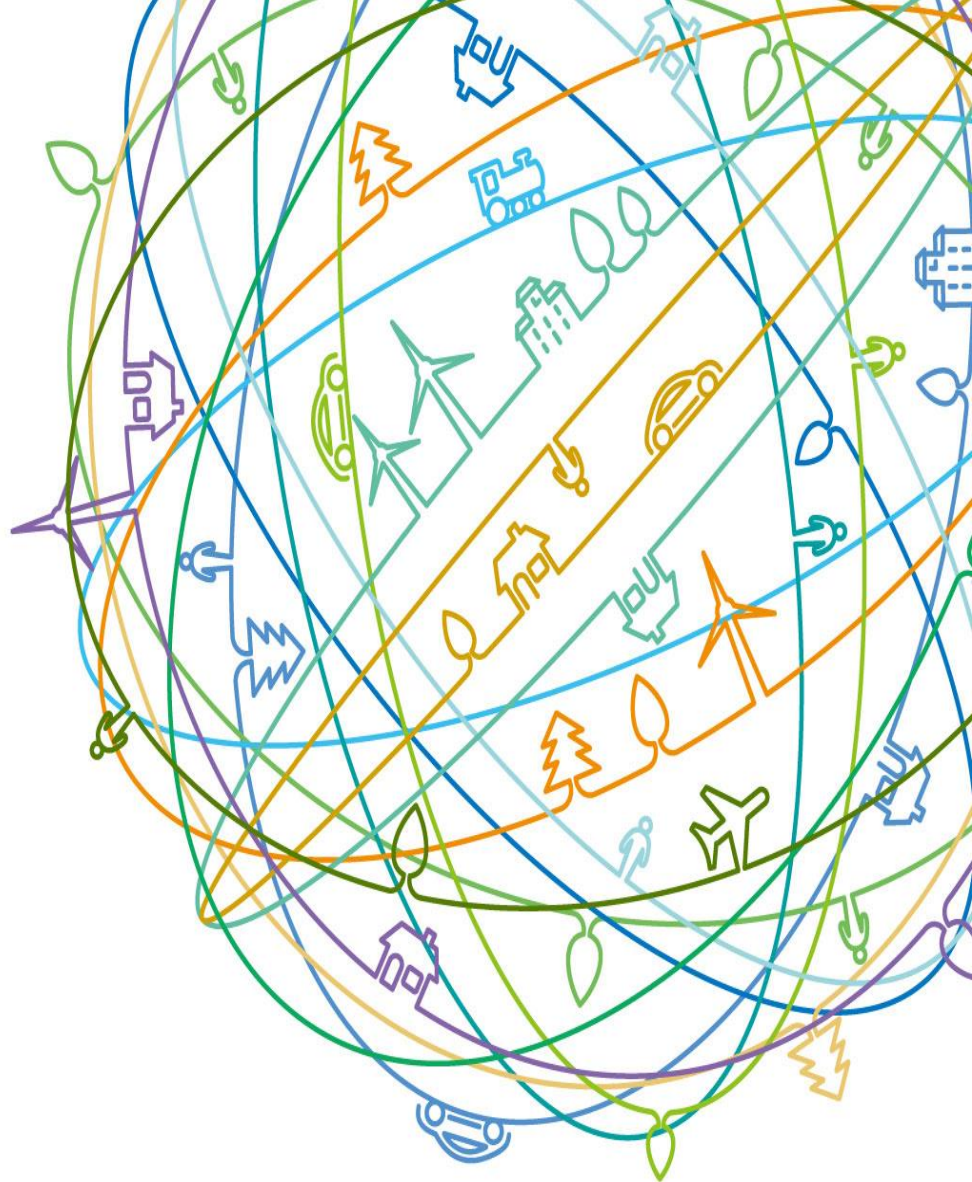


以信任的名义：- 区块链技术的技术的 的前世，今生与未来

Ken Huang
(343984)



目录

- 区块链是什么
- 怎么学
- 怎么用
- **区块链在华为的思考**
- **区块链的Killer APP 是什么**
- 区块链落地的痛点
- **其他问题**

真实的故事：信任的危机

民生银行30亿假理财案疑似窝案 多部门或联合造假。多名涉事员工被带走。



张颖同志先进事迹材料

中国民生银行北京管理部先进个人

我要留言

区块链：信任的机器

The
Economist

Topics ▼

Print edition

More ▼

The promise of the blockchain

The trust machine

The technology behind bitcoin could transform how the economy works





信任的第3方：支付宝



信任的第3方：密码学

区块链网络下的“去中心化”的方式：



起源

Carrier 9:05 PM

< Back About

Source: <https://bitcoin.org/bitcoin.pdf>
(2008)

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gnx.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

< >



从比特币开始追溯区块链



区块链的前生

2009-10-5, 有记录的最早比特币汇率

1比特币 = 0.00076 \$ = 0.005 ¥

2017-3-13

1比特币 = 1261 \$ = 7989 ¥



比特币创始人之谜

中本聪Satoshi Nakamoto

已积攒约100万个比特币。如全部转化为现金, 中本聪的净资产大约为数亿美元



跳出来的中本聪

澳Craig Wright公开表明中本聪身份
2016年2月与nTrust合作, 经 EITC 申请专利已公开54件, 计划400件, 预计售价10亿美元, 内容包括密钥、验证、钱包、网络扩展、安全支付、物联网操作系统
据悉目的是向谷歌等公司出售专利

提问

区块链主要解决什么问题？

各国政府对区块链的态度

美国：巨头布局

- 15年年底，各大金融机构都加大了区块链技术研究（IBM、JP摩根、伦敦证券交易所）
- 2016年6月，美国国土安全部加大区块链对政府应用

欧洲议会：对新技术持开放态度

- 16.2 欧盟委员会把加密数字货币放在快速发展目标领域的首位。
- 16.4 举办欧洲数字货币与区块链技术论坛（EDCAB）

俄罗斯：态度由强硬趋于缓和
16年初俄央行以比特币交易，主要是P2P交易和个人业务托管

韩国：自上而下地进行区块链创新

- 16.2，韩国央行鼓励区块链技术
- 同月，韩国唯一的证券交易所Korea Exchange（KRX）宣布开发基于区块链技术的交易平台。

中国：行业联盟迅速兴起

- 16.2，央行明确区块链技术价值
- 2015年12月区块链研究联盟，2016年1月，中国区块链研究联盟；2月，中关村区块链产业联盟成立；4月，中国分布式总账基础协议联盟（ChinaLedger）宣布成立

澳大利亚：多领域探索区块链技术

- 16.3 澳大利亚邮政用区块链技术在身份识别中的应用

迪拜：建立全球区块链委员会

- 16初成立联盟，有会员30名，Cisco、区块链初创公司，迪拜政府等
- 2016年5月30日，迪拜全球区块链委员会（GBC）举行了2016年行业主题会议，公布了7个新的区块链概念验证。包括：医疗记录、保障珠宝交易、所有权转让、企业注册、数字遗嘱、旅游业管理、改善货运。

从各国反应来看，区块链在逐渐被各家认可，并以金融为切入点进行研究，美国较为激进

IBM：将区块链作为公司战略，在多个行业推动应用

将区块链视为两根救命稻草之一，内部大力投入资源发展区块链

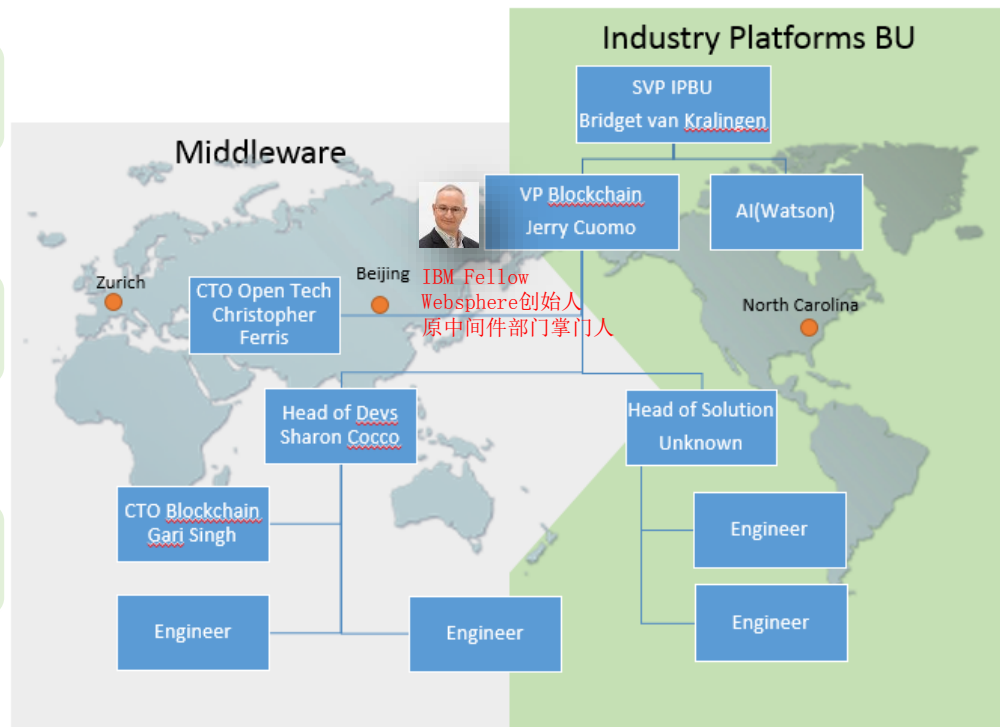
- 成立新的一级部门，由前GBS主管Bridget领导
- 区块链方面投入100-200专职人员
- 17年将追加40%区块链方面的投资

发展和引导产业

- 参加HLP，大力投入Fabric，推动其成为事实标准
- 在各个行业推动应用方案：供应链、物联网、医疗等
- 推销基于Mainframe大型机的区块链解决方案

创造客户

- 合作伙伴计划：据称有200-300家单位公司和机构都在寻找与IBM联合进行PoC验证
- 部分项目已经盈利



图：IBM内部区块链相关组织结构

“Blockchain is so profound it will do for trusted transactions what the internet did for information”. – Ginni Rometty, IBM CEO

区块链技术及应用生态系统

技术起源

- P2P网络
- 加密
- 数据库技术
- 电子现金

区块链1.0

- 分布式账本
- 块链式数据
- 梅克尔树
- 工作量证明

区块链2.0

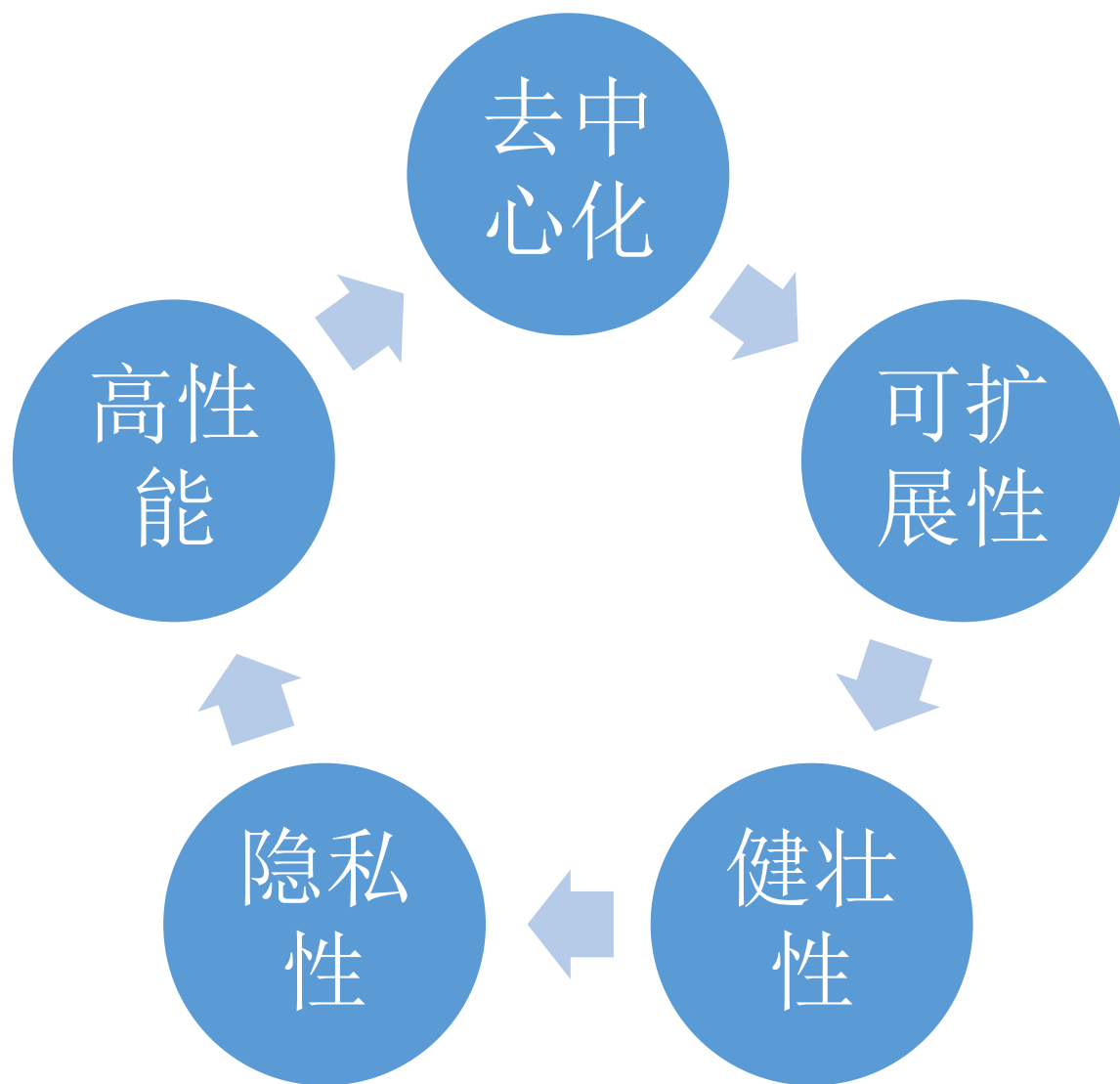
- 智能合约
- 虚拟机
- 去中心化应用

区块链
演进路径

区块链应用的生态系统



P2P网络的特征



数字签名原理

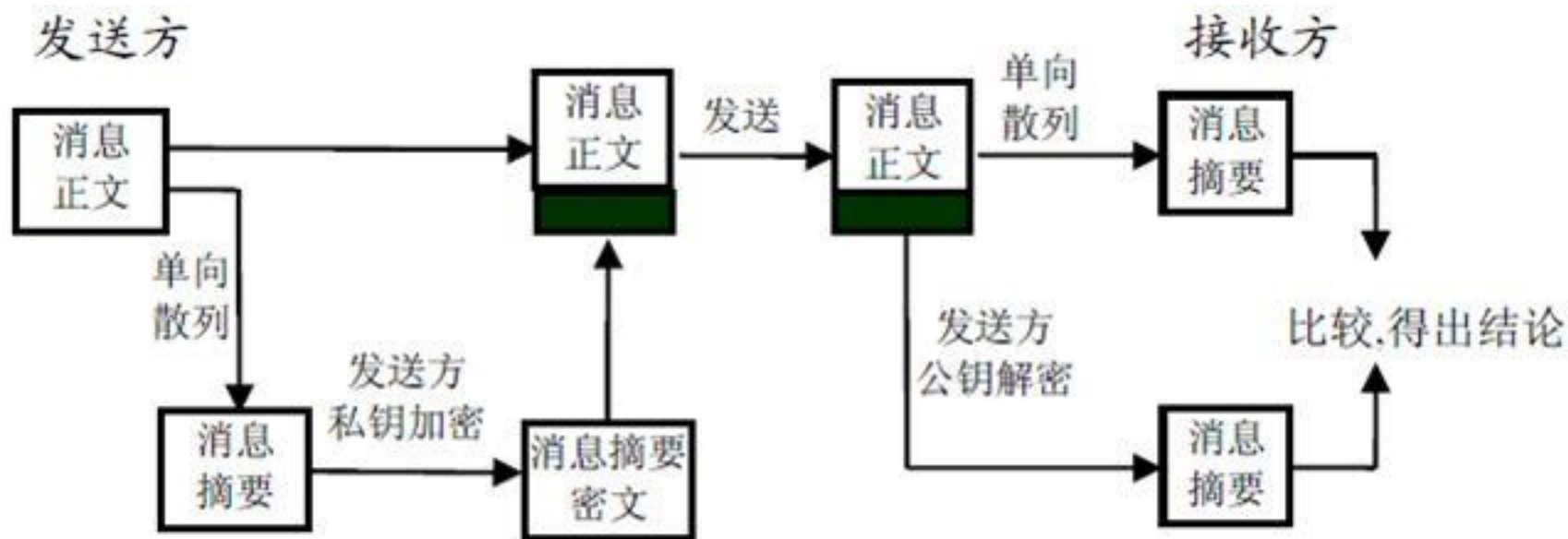


图 1 数字签名的基本过程

常见的共识算法

- POW
- POS
- DPOS
- BPFT

区块链类型及工作流程

区块链的不同类型及特性

公有链

- 任何人都可加入网络及写入、访问数据
- 任何人在任何地理位置都能参与共识

联盟链

- 授权公司和组织才能加入网络
- 参与共识、写入及查询数据都可通过授权控制，可实名参与过程，可满足监管AML/KYC

专有链

- 使用范围控制于一个公司范围内
- 改善可审计性

区块链如何工作？














A想要发送钱给B

这笔交易在网络上以一个“区块”作为代表

该区块广播给网络里的所有参与者

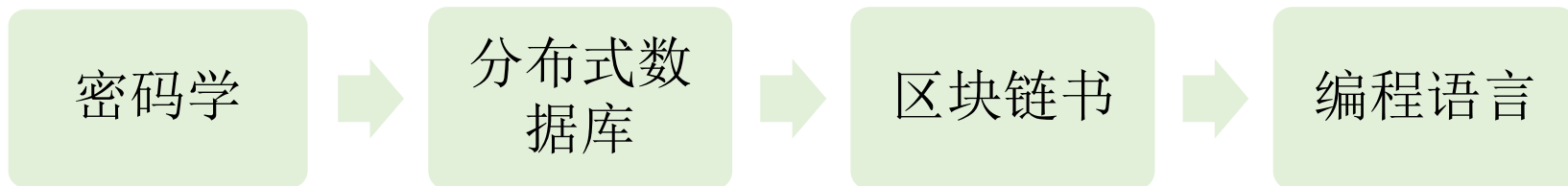


区块链 Top 10 币 (As of July 13, 2017)

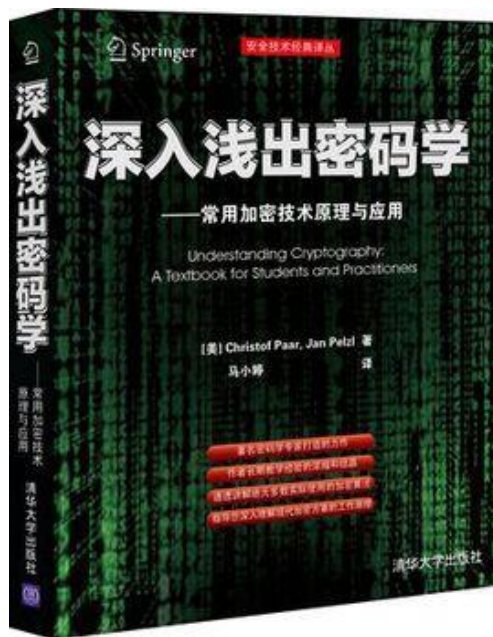
▲#	Name	Market Cap	Price	Circulating Supply
1	 Bitcoin	\$39,307,943,775	\$2390.24	16,445,187 BTC \$1
2	 Ethereum	\$20,207,141,901	\$216.70	93,247,665 ETH \$1
3	 Ripple	\$7,822,088,115	\$0.204278	38,291,387,790 XRP * \$
4	 Litecoin	\$2,434,034,047	\$46.84	51,968,632 LTC \$
5	 Ethereum Classic	\$1,760,180,789	\$18.82	93,506,770 ETC \$
6	 Dash	\$1,288,959,243	\$173.64	7,423,256 DASH
7	 NEM	\$1,163,619,000	\$0.129291	8,999,999,999 XEM *
8	 IOTA	\$611,621,741	\$0.220045	2,779,530,283 MIOTA *
9	 Monero	\$572,778,125	\$38.77	14,774,394 XMR
10	 BitConnect	\$403,595,908	\$58.43	6,907,163 BCC
11	 EOS	\$391,437,807	\$1.83	214,173,131 EOS *
12	 Stratis	\$364,967,131	\$3.71	98,461,204 STRAT *
13	 BitShares	\$348,647,534	\$0.134262	2,596,770,000 BTS *

Source: <https://coinmarketcap.com/>

区块链技术怎么学习？



密码学



作者: Christof Paar / Jan Pelzl

出版社: 清华大学出版社

原作名: Understanding Cryptography: A Textbook for Students and Practitioners

译者: 马小婷 出版年: 2012-9 页数: 351

定价: 59.00元

ISBN: 9787302296096

分布式数据库



<https://item.jd.com/12010439.html>

区块链书



区块链三类开发者

- 一类是开发基于区块链的Web或移动App，这种开发者所需要的技能与今天的Web和移动开发者相同。
- 第二类开发者是开发智能合约的。这类开发者使用类似Solidity这样的智能合约语言，或者直接用Go、Java、Python等语言开发。开发智能合约所要求的语言和算法技术水平不高，什么并发、多线程之类的东西一般用不到，普通开发者均可胜任。但是智能合约的难点在于业务与安全。本质上智能合约就是以代码写成的商业合同，必须对于业务有非常清晰的认识，对于安全有着深刻的理解，才能够写出正确的智能合约。
- 第三类开发者，就是区块链核心应用系统和核心平台的开发者。这部分人当然必须是技术高手，按现在通俗的说法，得是后端专家。从语言上讲，C++、Java、Python、Go、JavaScript都有可能要触及。从基础知识来说，要求对密码学、分布式系统、网络编程、系统架构和部署都有相当程度的理解和实践经验。这种开发者显然将是区块链技术浪潮当中的弄潮儿，也将是最大的受益者之一。

区块链开发人才短缺 工程师年薪超50万英镑

区块链开发人才短缺 工程师年薪超50万英镑



区块链中文网

百家号 | 06-16 16:17

关注

据英国Financial News网站报导，区块链(blockchain)技术据信可为金融服务业者带来突破性变革，银行、金融科技新兴公司和顾问机构争相重金礼聘人才，顶尖区块链开发工程师可以日进斗金，年薪达到50万英镑(约合430万人民币)。



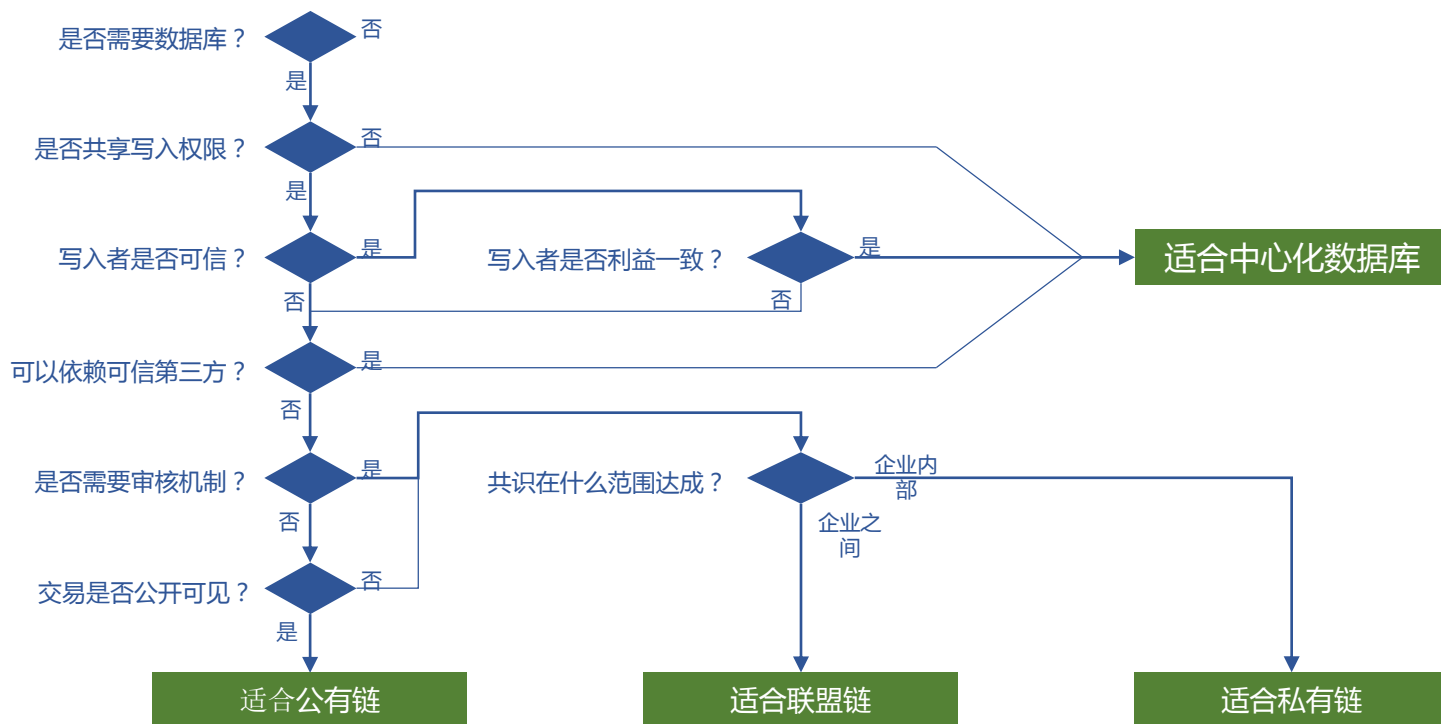
区块链技术兴起让该领域的人才炙手可热，产业专家表示，顶尖区块链开发工程师极为稀少，他们的年薪可高达25万至50万英镑。

专业人才仲介公司Liberam创办人柏吉斯-凯利(Richard Burgess-Kelly)表示：“区块链、人工智能和机器学习等新领域的人才十分短缺，如果你拥有区块链相关领域的博士学位，就能日进斗金。”

柏吉斯-凯利表示：“拥有区块链博士学位的人才1天便可轻松赚进500至1,500英镑。”

区块链怎么用？

怎么用？



两个要素：

- 需要数据读写
- 有多个参与者
- 我们不知道！

区块链在华为有没有成功的可能？

1. 上下不碰的困境。
2. 学习IBM？
3. 软硬兼施是华为创新产品的必要条件吗？
4. 我们区块链的创新环境是什么？
 - 层层汇报？
 - 胶片文化？
 - Lean Startup!
 - 需要说“人话”的“骗子”：王坚！
 - 200 亿美金的投入？
5. 区块链的领跑者

区块链的Killer App是什么？

为什么需要身份链

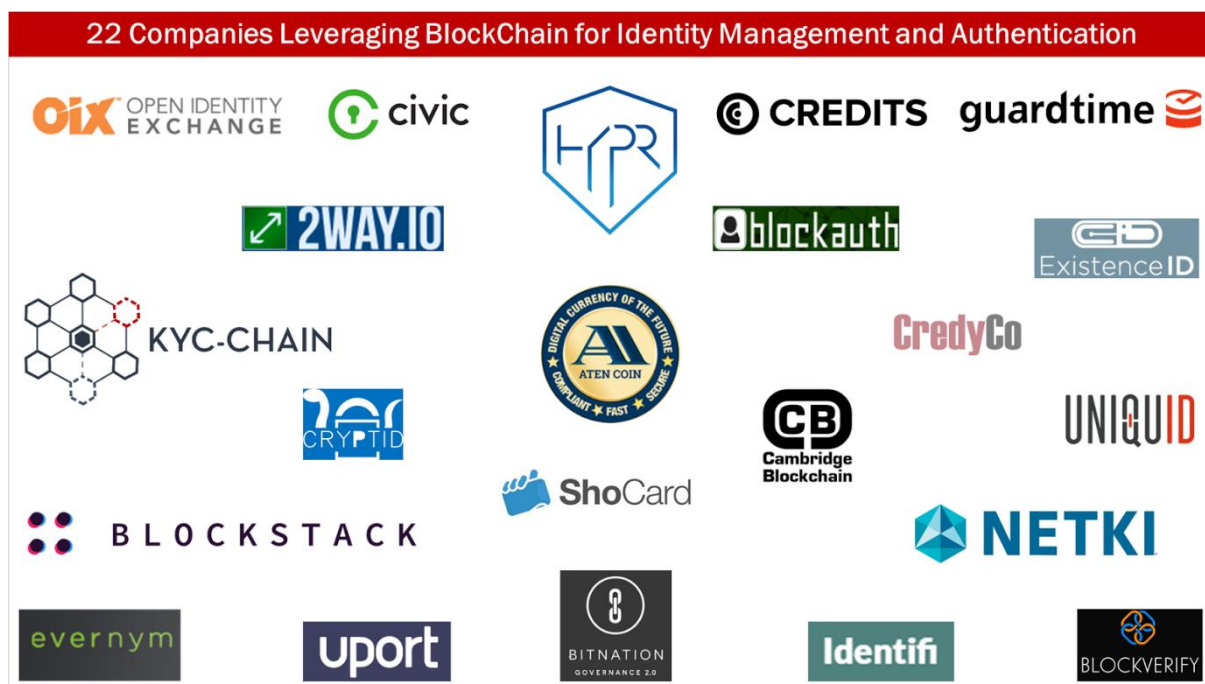
- 区块链的基础
- KYC, AML
- 用户画像和智能钱包
- 智能投资顾问
- 身份盗窃保护（Civic）
- 欺诈检测（例如贷款欺诈）

身份链可以解决的问题

传统身份管理系统的问题	区块链的解决方案	华为的优势
Fragmented Identity	Store Encrypted on the Ledger Store on Mobile Device	BAAS with Security Mobile Device
User has no control	Self-Sovereign Identity	Mobile Device
Password	PKI Biometric	Mobile Device
Identity proofing is expensive	Identity proofing result can be recorded on the Blockchain	Work with Carriers/Banks on a ecosystem
Identity is static, rigid and not flexible	With Smart Contract, Identity can be dynamic and flexible to enable ABAC using Smart Contract.	Work with standard body (such as EEA)

身份链项目和公司简介

22家身份链公司



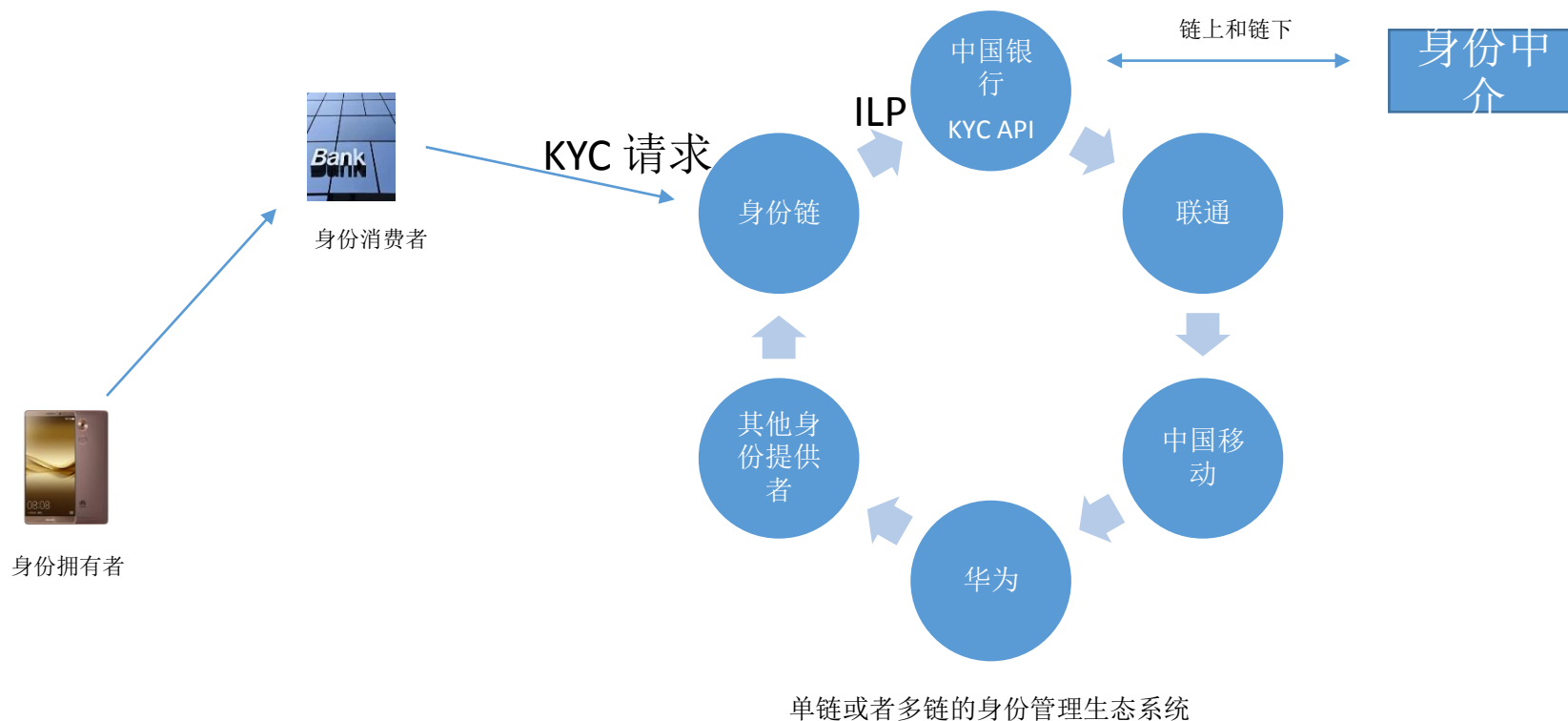
贵阳市的“身份链”

- 贵阳市有关部门将“身份链”项目建设列为贵阳市基于区块链、大数据技术的社会诚信体系建设的基础设施建设内容。贵阳市选取清镇市作为试点，用案例诠释身份链对不同场景下身份的管理，使得全链网自动捕捉个性化场景化诚信痕迹全景式呈现。而且清镇市“诚信农民”的线下实践已开展多年，广受关注和好评，也有一套评价方法具备操作可行性。结合贵州省省情以及中国乡土实际，对于农民的诚信评价颇具价值，对全球也具备借鉴意义。
- “身份链”一期原型：终端采集器、基于受理数字资产钱包及账户体系等4-5个独创性的技术。

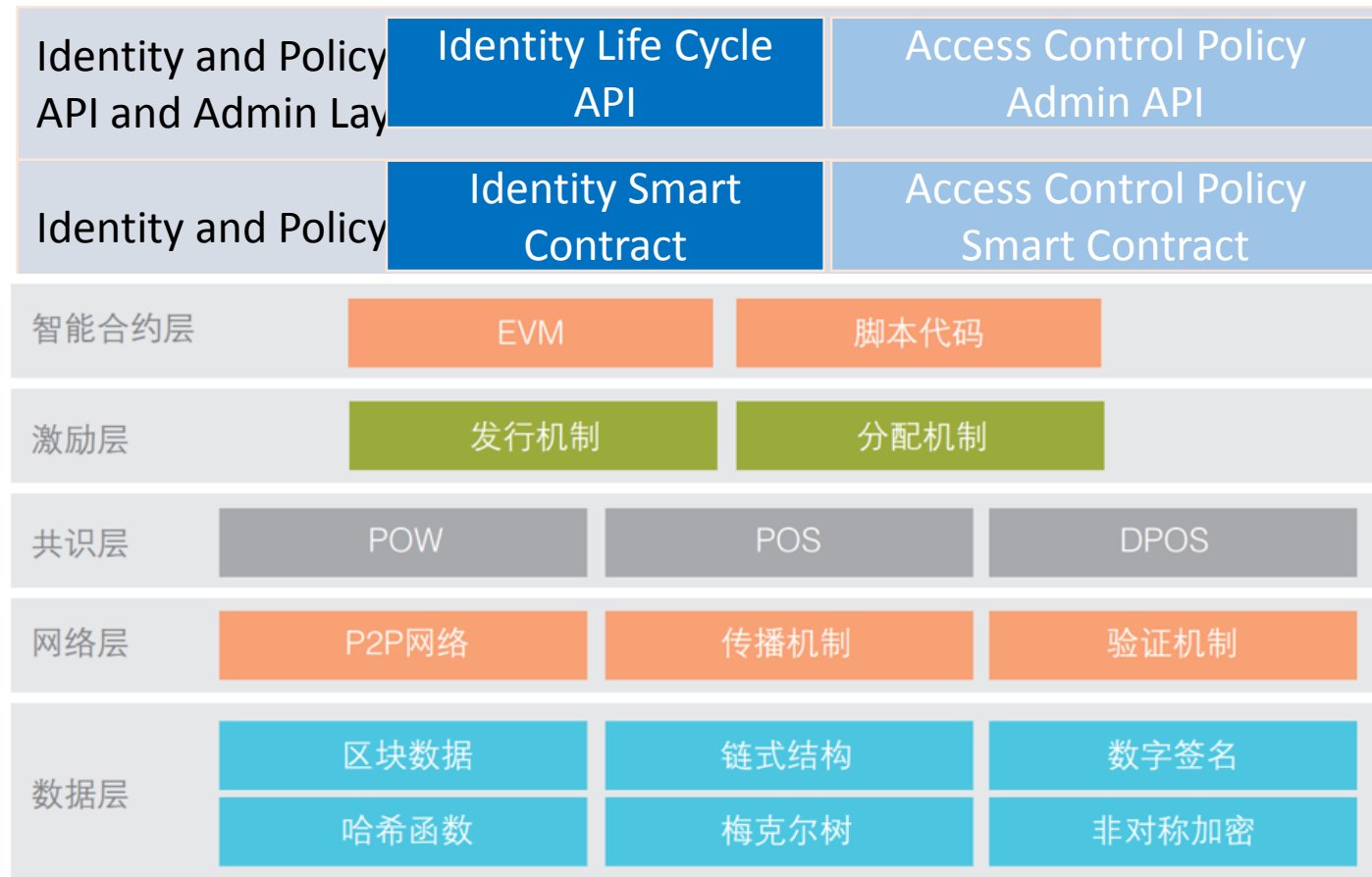
身份链的技术要点

- 总体架构
- 分层架构
- 数据架构
- 几个应用场景

High Level Architecture



Overall Layered Architecture



身份链的数据模型

Key Idea: Smart Contract on Blockchain

- Have states
- APIs (public and private API)
- Given RAM and CPU resource for the API to execute
- Needs strong security or formal verification before store it on blockchain
- May need some capability of updating/deleting a smart contract. (right to forgotten)
- Is the key for Blockchain Identity implementation.

Blockchain Identity Eco-System

- Identity Oracle: perform identity proofing, identity attribute attestation.
- Identity Provider: the Blockchain with Identity Smart Contract
- Identity Consumer: users and/or systems who need identity to perform a task.
- Owner of the Identity: The actual person or entity who owns the identity (using Private Key to prove ownership).

Identity Smart Contract

- The attribute of the identity can be attested and inserted by Identity Oracle under Owner's request and approval.
- The attribute can be encrypted
- Only the owner of identity can decide which Identity Consumer has access to which Identity attribute.

Identity Life Cycle API

- CRUD of identity and Attributes
- Can support Rest API
- Encrypt/Decrypt Attributes.

Access Control Policy Smart Contract

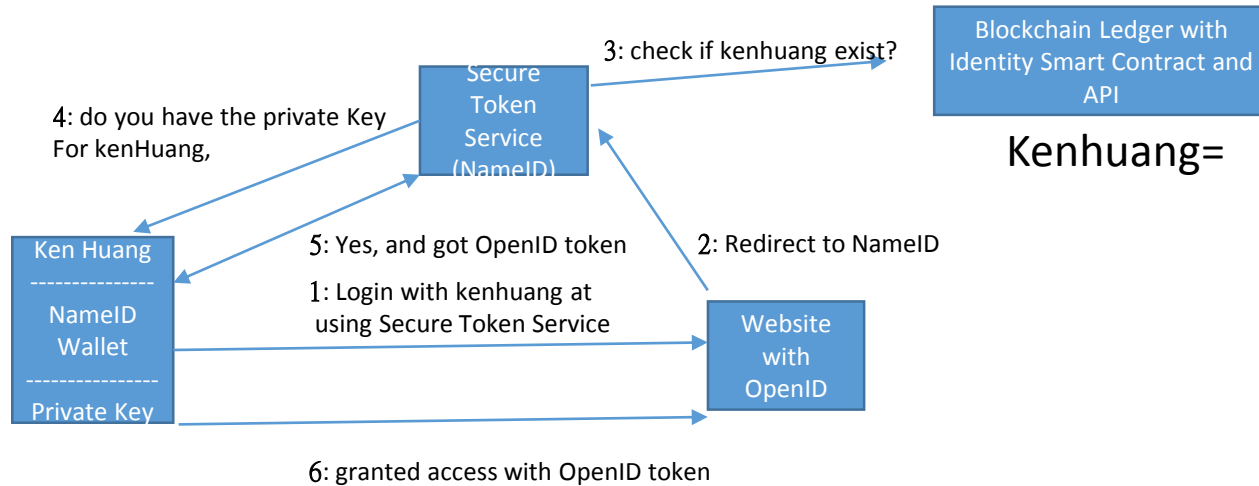
- Group Smart Contract
- Role Smart Contract
- Resource Smart Contract (similar to ARN in AWS).
- Managed Access Policy Smart Contract(examples)
 - Read/Write Access to Identity Attributes via HTTPS and Oauth
- Customized Smart Contract

Access Control Policy Admin API

- CRUD of Access Control Policy
- CRUD of Resource Tags
- Attach/Detach Policy to User/Group/Role API
- Can support Rest API
- Example: create a policy: grant access to Bank of China to access my Driver's license number.

身份链的几个应用场景

Use Case 1: Sequence Diagram for User Access to Website with Blockchain Identity



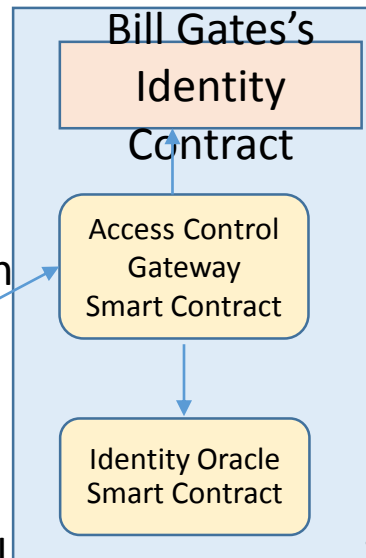
Use case 2: Create a human identity by Identity Oracle



1: I am Bill Gates, here is my Driver license. I need an identity on the blockchain

Identity Oracle (can be a government organization)

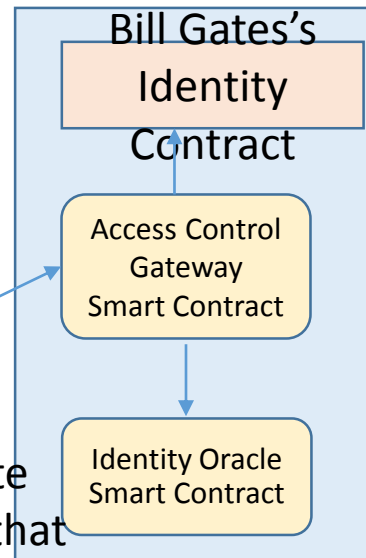
2: I verified bill
Can I create Bill?



4: Create Bill Gates and send Bill his private Key, only record the hash of Bill's private key

3: Check if this Oracle can create Identity
(assumed the oracle
Authenticated previously)

Use case 3: Identity Oracle attest an attribute for identity



1: I am Bill Gates, I was CEO of Microsoft. Can you attest it and record it on the blockchain

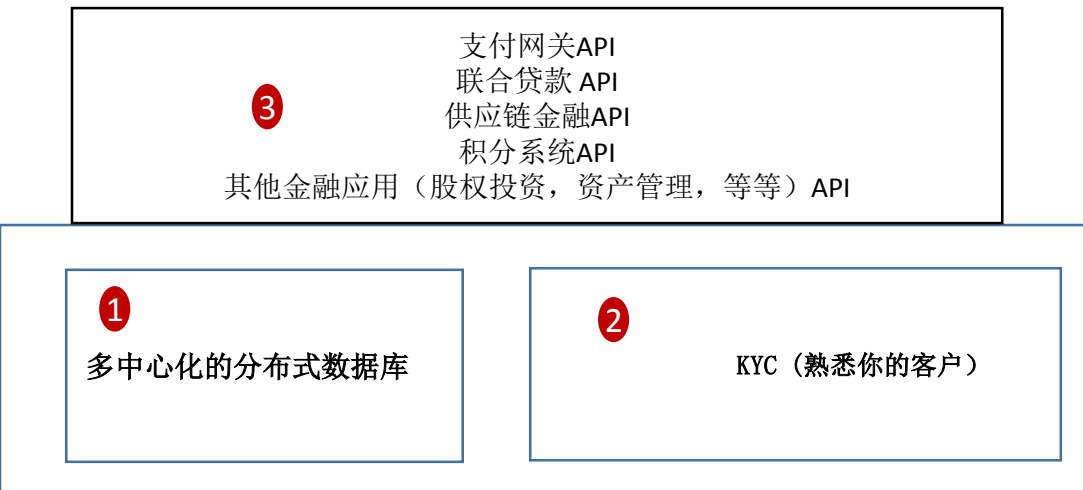
Identity Oracle (can be a government organization)

2: I need update Bill and attest that He was CEO of M.S.

4: Bill Gates's identity is updated to state that he was CEO Of Microsoft

3: Check if this Oracle can attest attributes (assumed the oracle Authenticated previously)

华为区块链金融产品的初步思路



保证数据在交易各方之间**公开透明**，在整金融行业**形成一个完整且流畅的信息流**，确保了参与各方及时发现金融系统运行过程中存在的问题，并针对性地找到解决问题的方法，**提升整体效率**。

区块链所具有的数据**不可篡改**和时间戳的**存在性证明**的特质，很好地解决金融行业体系内各参与主体之间的纠纷，**实现轻松举证与追责**

区块链可以消除中间环节从而**减少费用**

1 多中心化的分布式数据库

- 保证数据在交易各方之间**公开透明**
- 交易各方可以协同工作，提高整体效率

2 KYC (熟悉你的客户)

- **减少KYC的成本**
- 提高安全
- 优化客户经验
- 形成的KYC生态系统。

3 金融BAAS API (aPAAS)

- 提高SDK和API，促进金融区块链生态的形成
- 减少开发的费用

区块链常见问题

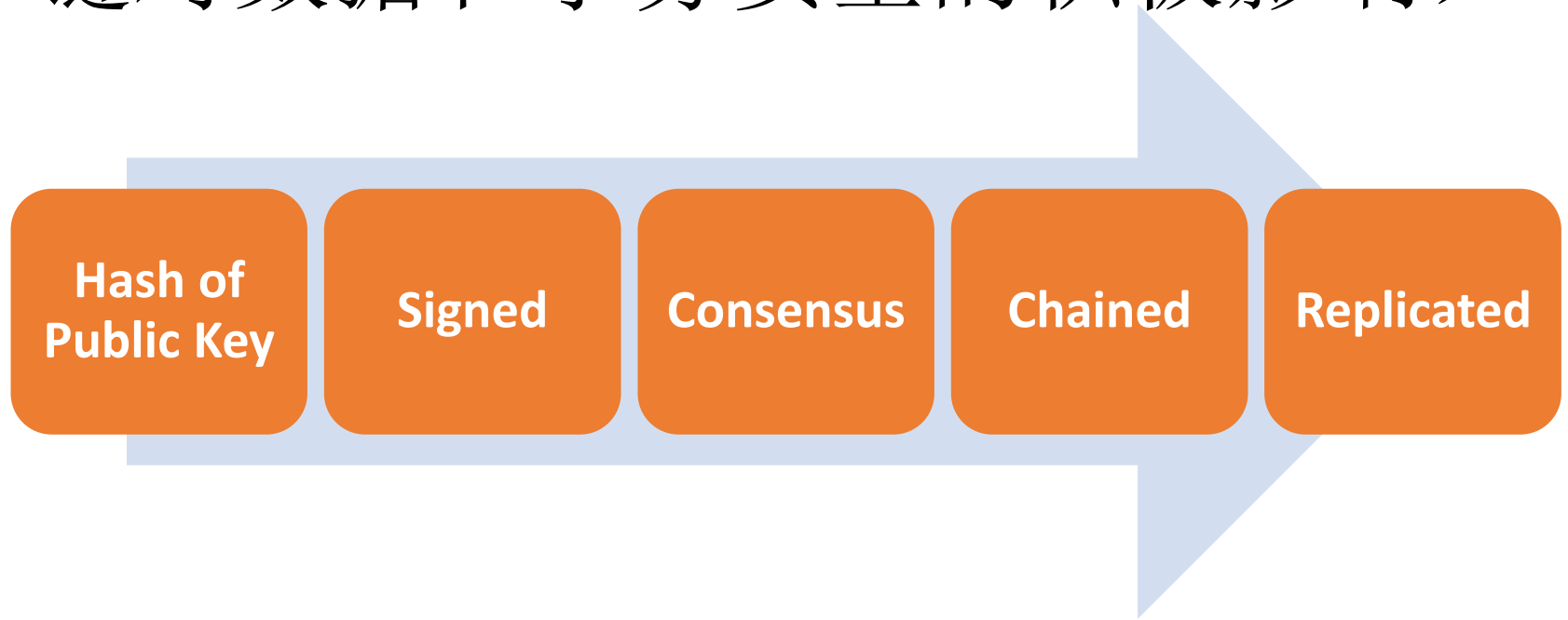
- EOS vs. ETH
- 什么是ICO?
- Polkadot 是什么?
- 去中心化的特性是否对中心化机构不利?
- 区块链是低效服务吗?
- 区块链是否没有隐私?
- 不学习区块链我会不会没有工作?

区块链的安全问题

Table of Contents 目录

- 区块链对数据安全的积极影响
- 从安全3要素看区块链
- 工信部白皮书区块链2.0技术架构和对应的安全层次
- 两个典型的区块链安全问题简单剖析
- 总结

Positive impact of BlockChain for Data and Transaction Security (区块链对数据和事务安全的积极影响)



从安全3要素看区块链: Confidentiality(保密性)

Hash of Public Key

HyperLedger Transaction Certificate (full Confidentiality of the user identity)

Encryption of Data using Zero knowledge (零知识)

- Zcash using zk-SNARK for bitcoin like transaction
- Hawk using zk-SNARK for smart contract

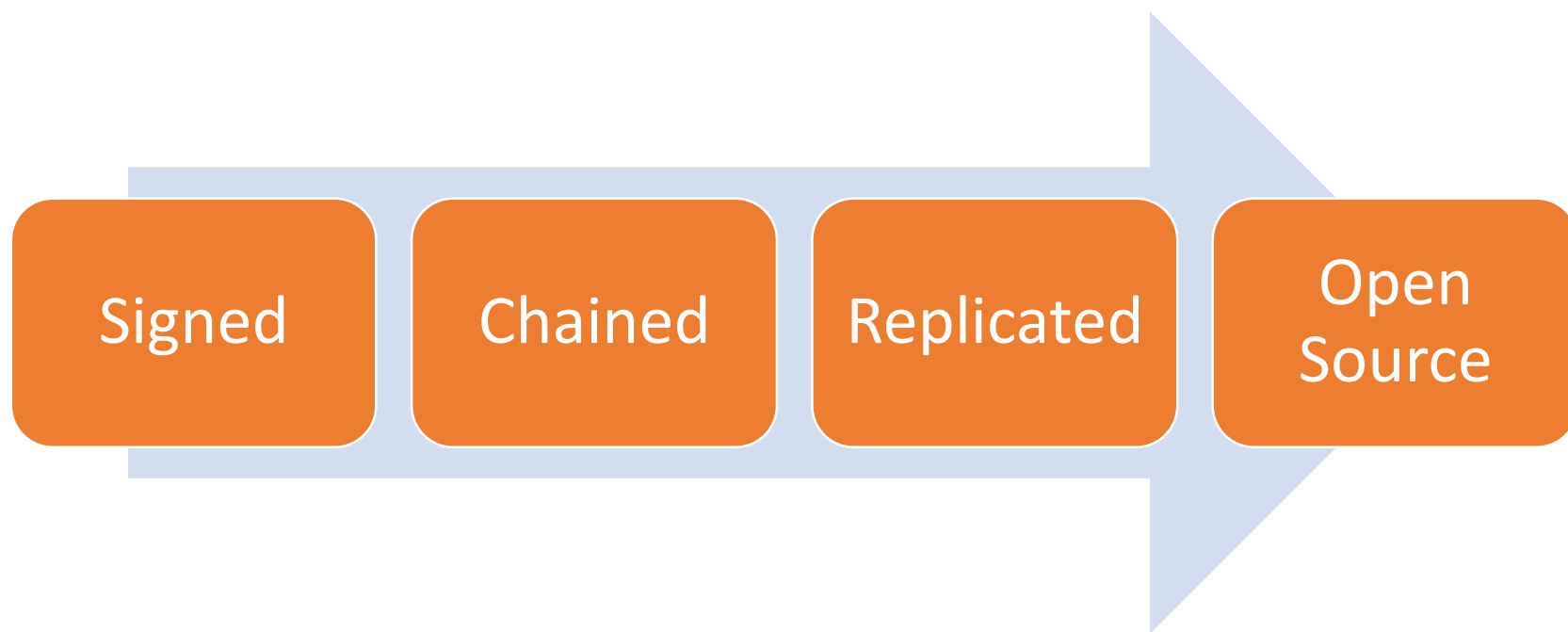
Data invisibility (不可见) via State Channel

- Lightning network for Bitcoin
- Raiden Network for Ethereum

Fungibility (同等性) of zcash

Homomorphic encryption (同态加密)

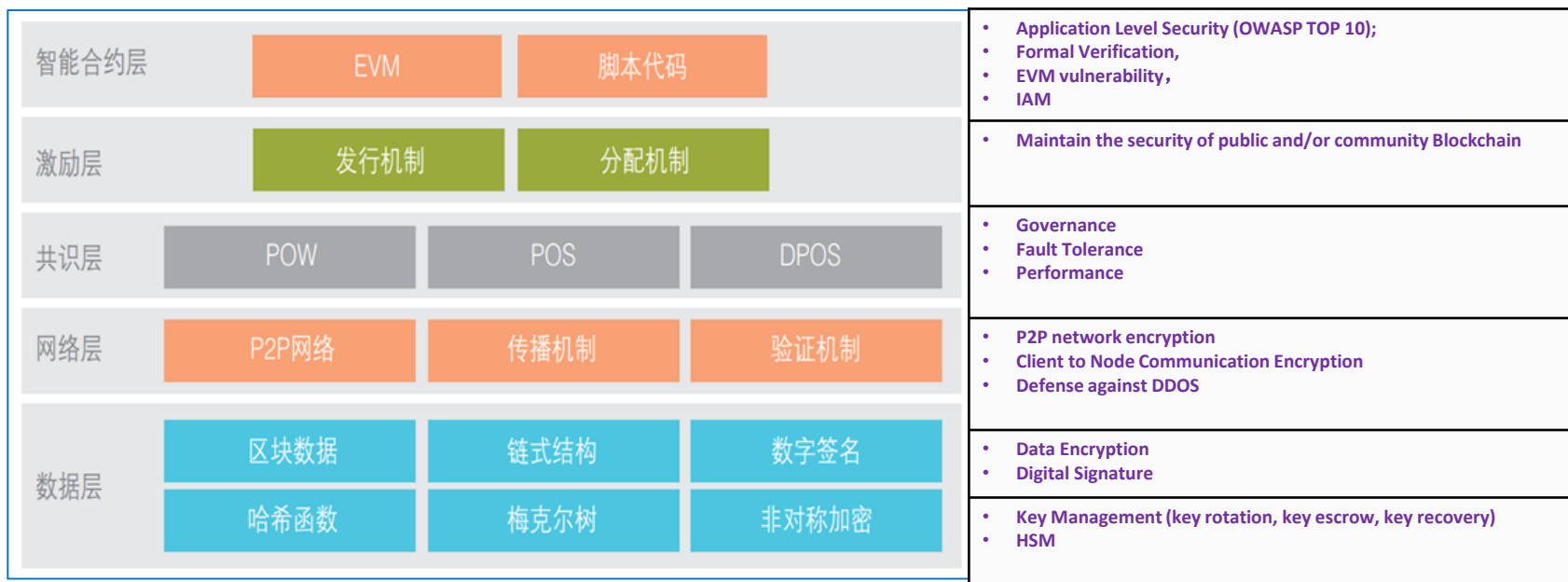
从安全3要素看区块链: Integrity(完整性)



从安全3要素看区块链: Availability(可用性)

- Each Transaction (or Data) is replicated (availability)
- But what about the latency?

工信部白皮书区块链2.0技术架构 和对应的安全层次



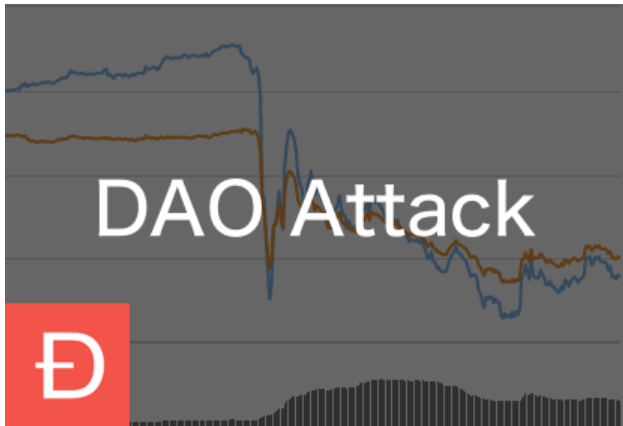
工信部白皮书区块链2.0技术架构

对应的安全层次

Top 8 安全控制

1. 身份管理
2. 应用层源代码安全检查
3. 智能合约安全检查
4. 节点的安全加固
5. 数据加密（链上和链下， 国密算法）
6. 数据传输的加密
7. DDOS
8. Key Management

DAO(Decentralized Autonomous Organization)分布式自治组织 Attack 的简单剖析



- The basic idea is this: the DAO smart contract has a recursion program which does not terminate correctly. The caller of the program can call the recursion program again without withdrawing the ether. As such, the hacker was able to accumulate the total ether to be withdrawn until a large sum (\$50 millions in virtual currency) by recursively calling the program.
- The problem can be mitigated if
 - Recursive program is checked before deployed
 - Formal verification.

Bitfinex 安全问题的简单剖析



INVISIBLE COMPANY

The \$65 million Bitfinex hack shows that it is impossible to tell a good bitcoin company from a bad one

- Bitfinex user has their own set of keys created on the platform, using a 2-of-3 key arrangement whereby Bitfinex held two of the keys (including one offline) and BitGo used the third to co-sign transactions.
- Bitfinex keys got stolen by hacker. BitGo trusted withdraw request from Bitfinex and signed the request. **\$65 millions** got stolen.
- The security breach could have been mitigated if
 - Bitfinex use HSM for storage of private keys.
 - BitGo limit the withdraw amount.

总结

区块链的5个安全属性

区块链的5个安全层次和8个Top安全控制

区块链交易APP的安全问题

Thank you

www.huawei.com

Copyright©2014 Huawei Technologies Co., Ltd. All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

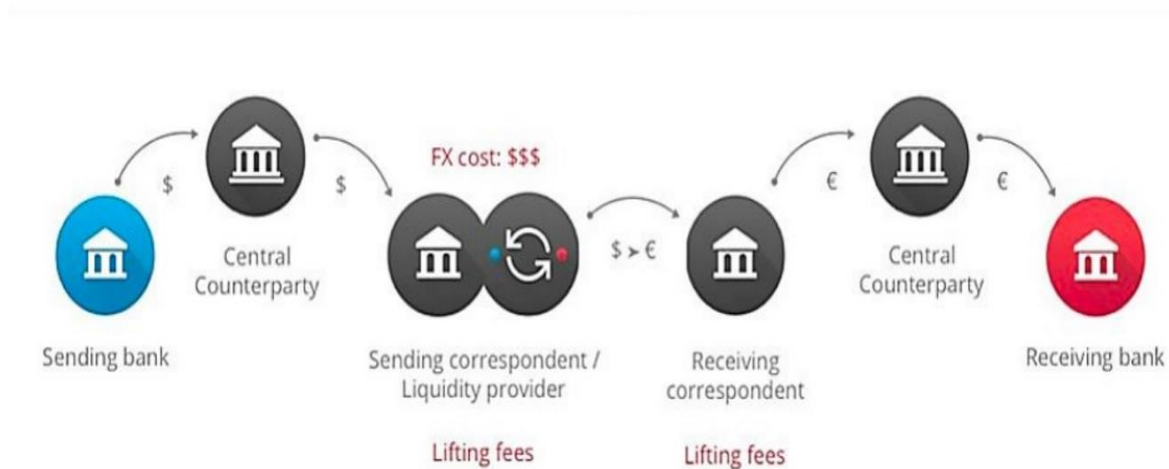
英格兰银行 / Ripple “Proof of Concept” 结果7月10号发布

英格兰银行 / Ripple "Proof of Concept" 结果今日发布

Jul 10, 2017 | Ryan Zagone



今天的FX



2-5 Days of Settlement Time For FX Transaction

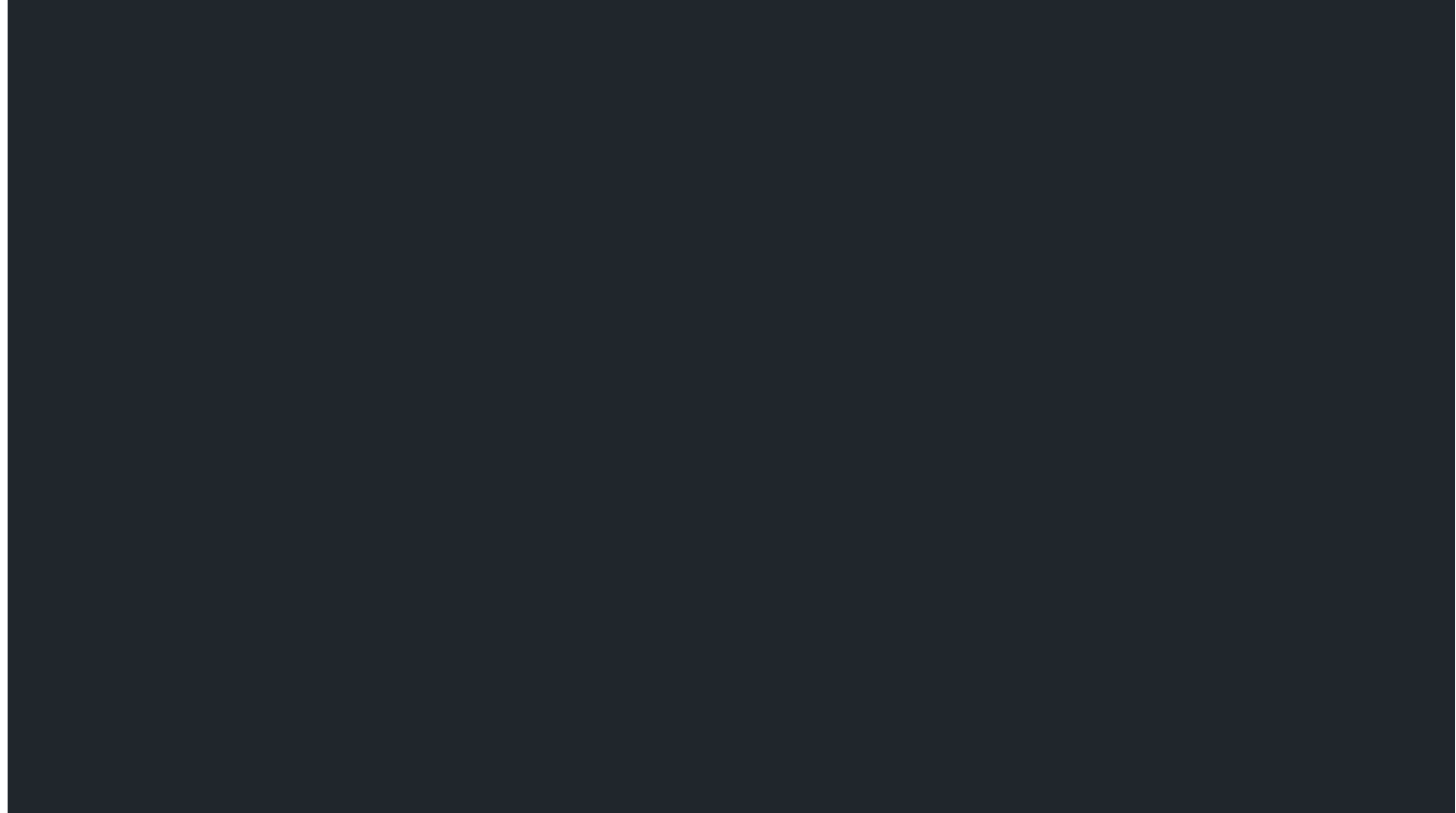
趋势： Fast Payment Task Force (USA) and PSD2

- Fast
- Small
- Transparent
- Open
- No Fixed Cost

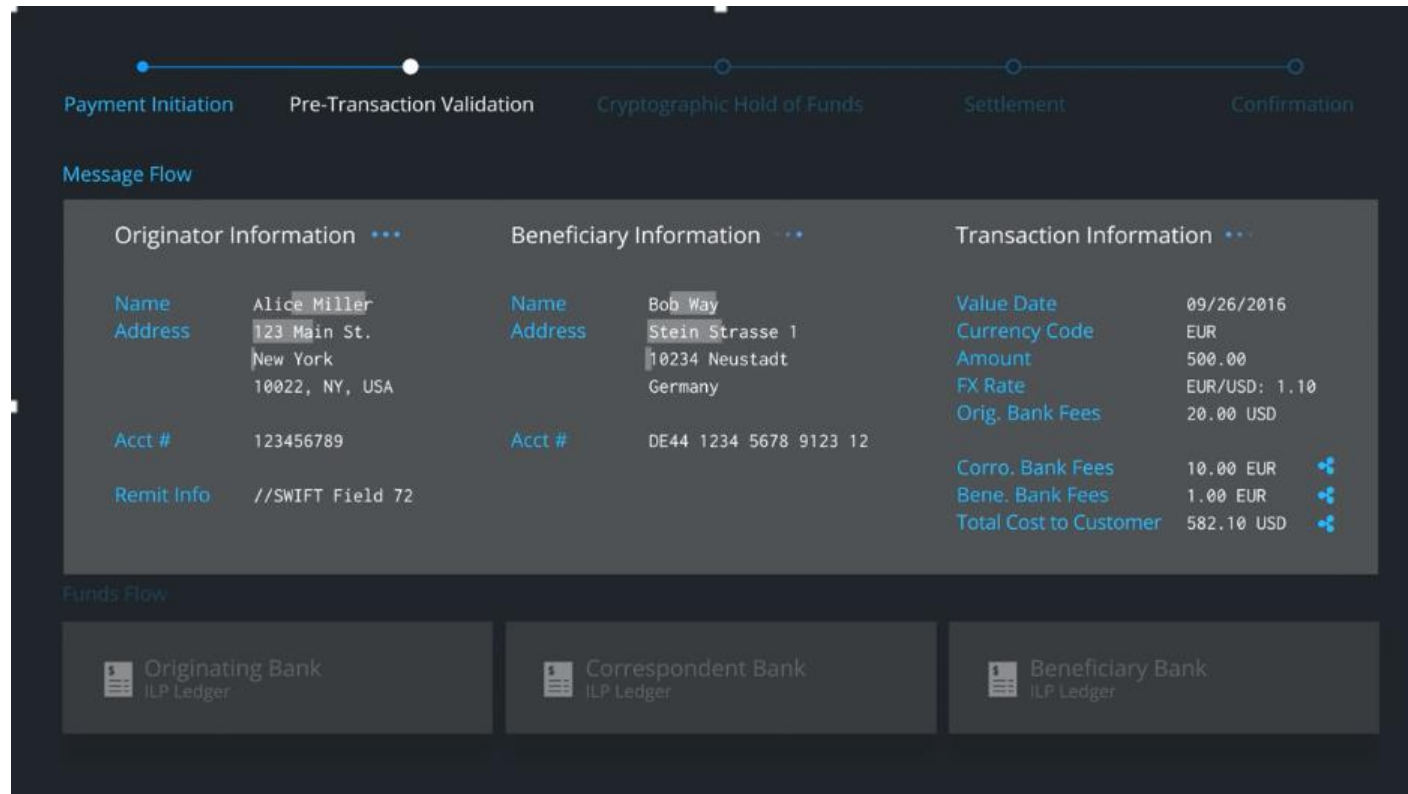
为什么不可以共享一个账本？
==》为什么不可以有一个账本之间的
协议？



How Ripple works (example using Correspondent Bank)



Typical flow of Cross-Border payment via Ripple Network



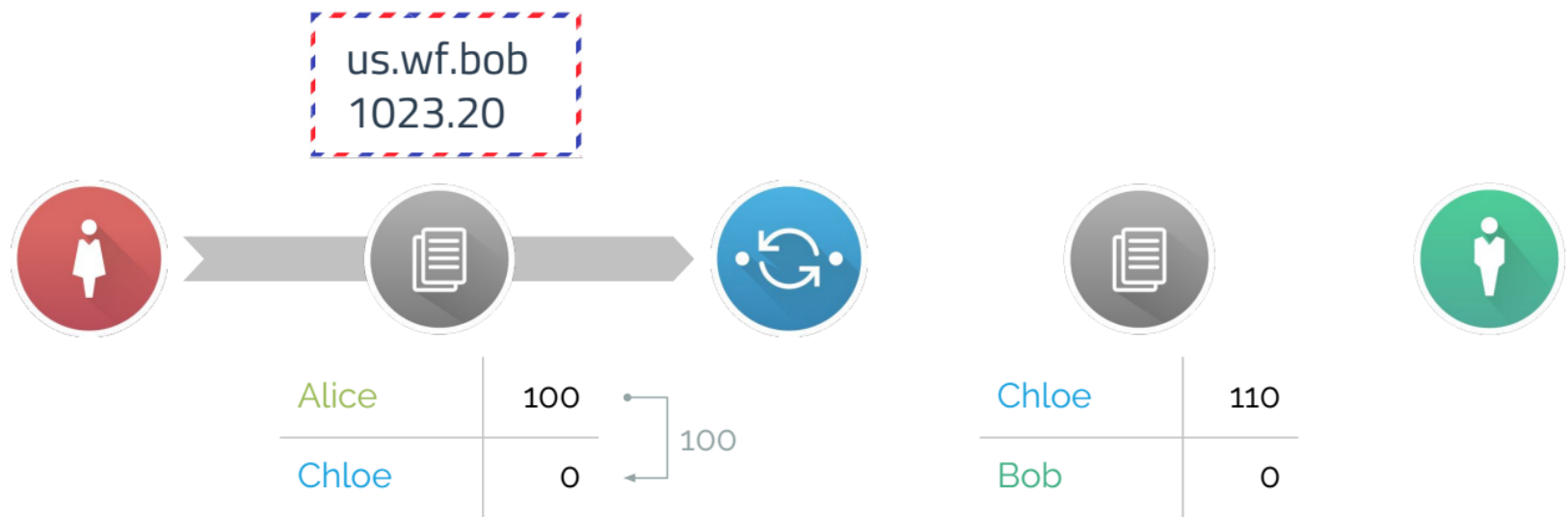
Ripple 的 Message Packet

Enabled By a Simple Packet Format

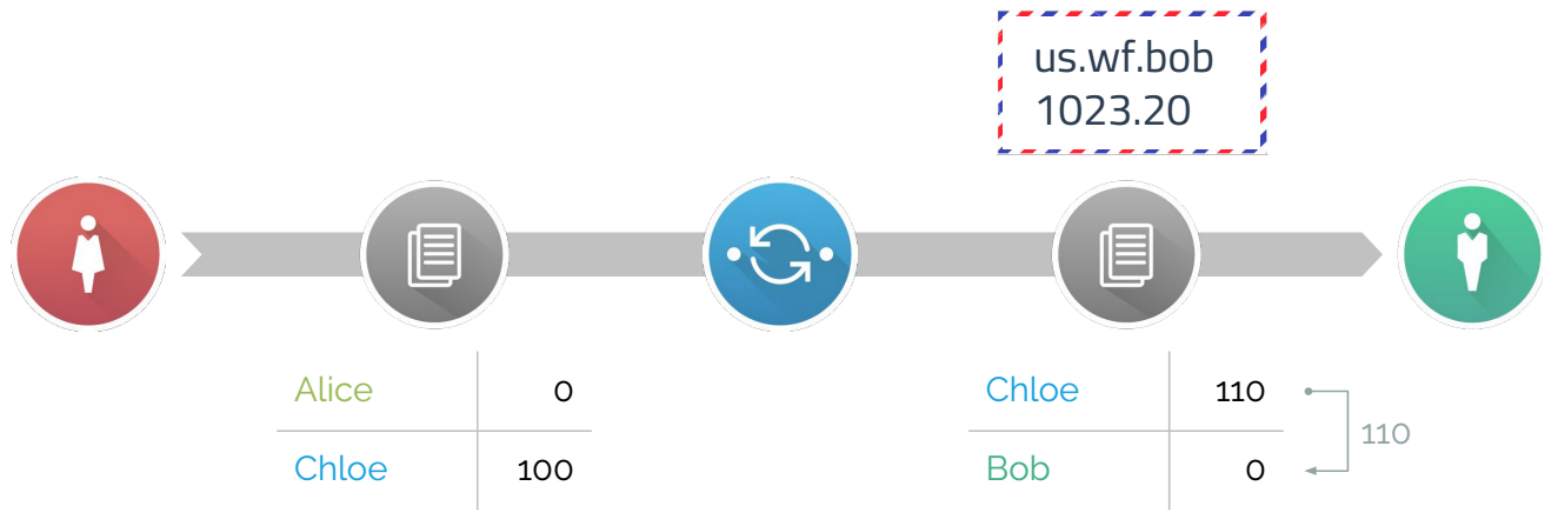
```
address:    "us.wf.bob"  
amount:     "1023.20"  
expiry:     "2016-07-06T09:00:10Z"  
condition:  "cc:0:3:4a7DEpj8f9..."
```



Sender Attaches Packet to Local Transfer



Connector Forwards the Packet via Another Transfer



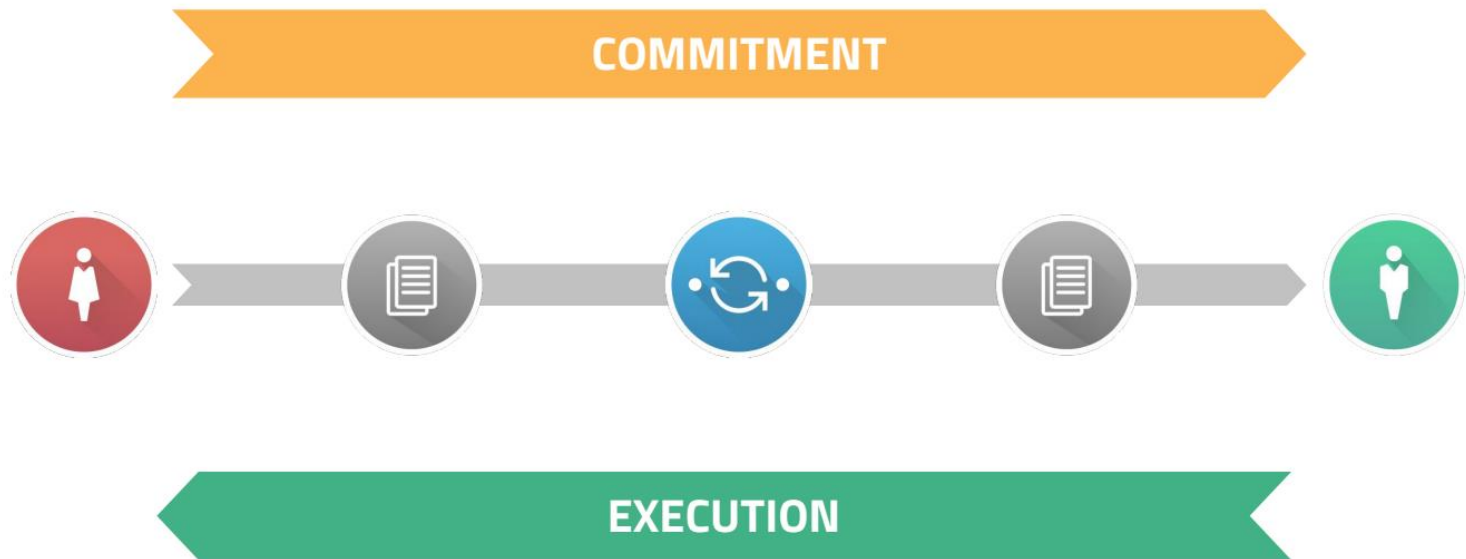
Paths Can Be Short



Or Long

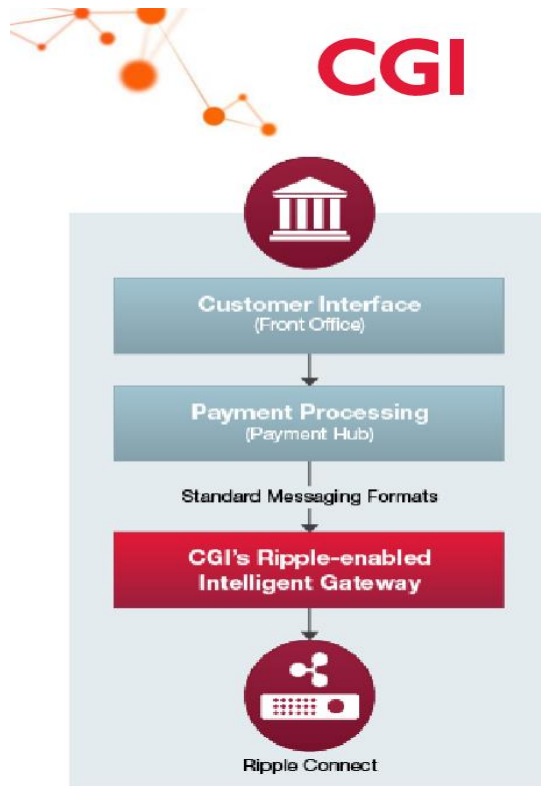


Transfers Are Committed L2R, Executed R2L



传统金融应用程序如何连接到Ripple?

CGI Ripple-enabled Intelligent Gateway



- Provides a **transformational wrapper** around legacy systems to isolate these rigid environments and allow flexible access to new protocols and services.
- Rules-driven, message-based **routing**, enrichment and **validation** also work to future proof the payments ecosystem
- Message enrichment and routing to compliance systems for **AML screening**
- Allow faster implementation of

Ripple现状

Ripple 收到9千3百万的投资， 96 亿美金的代币（2017/7）



Industry	Computer software
Founded	2012 ^[1]
Founder	Chris Larsen, Jed McCaleb
Headquarters	San Francisco, California
Area served	Worldwide
Key people	Ryan Fugger (Concept Originator) Alan Safahi (Advisory Board) David Schwartz (Chief Cryptographer) Ken Kurson (Advisory Board) Brad Garlinghouse (Chief Executive Officer)
Products	Ripple Payment and Exchange Network
Number of employees	150 (2016) ^[2]
Website	Ripple.com

Total Equity Funding \$93.6M in 7 Rounds from 27 Investors

▲#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$42,540,128,581	\$2588.79	16,432,437 BTC	\$745,198,000	-0.22%	
2	 Ethereum	\$24,974,693,235	\$268.35	93,067,610 ETH	\$602,081,000	-0.73%	
3	 Ripple	\$9,695,494,263	\$0.253203	38,291,387,790 XRP *	\$44,529,200	-0.75%	

Global Payments Steering Group (GPSG 6+1)

- Bank of America Merrill Lynch,
 - Santander (西班牙國際銀行)
 - UniCredit (意大利裕信銀行)
 - Standard Chartered
 - Westpac Banking Corporation (澳大利亞西太平洋銀行)
 - Royal Bank of Canada
-
- The Bank of Tokyo-Mitsubishi UFJ (BTMU, 東京三菱銀行) joined September, 2016

日本SBI Remit公司，泰国的SCB以及Ripple公司国际汇款系统上线



日本和泰国之间实现了快速而便捷的国际汇款

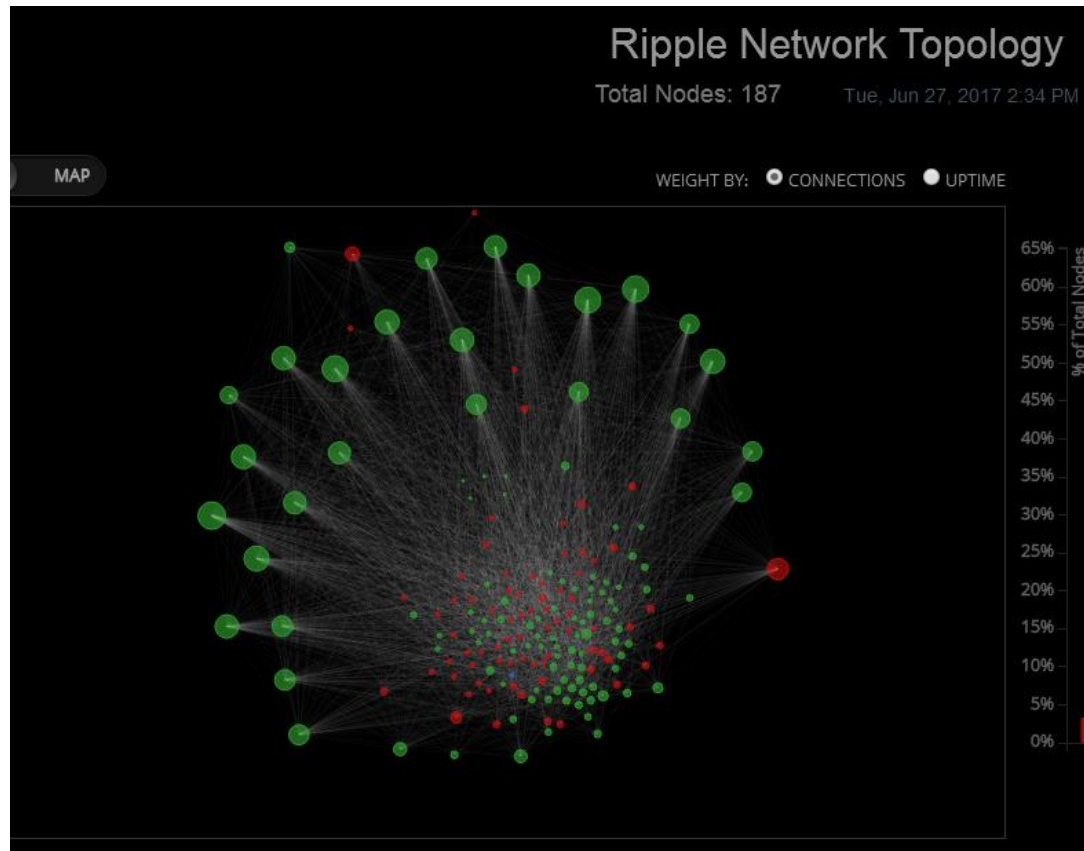
客户名单



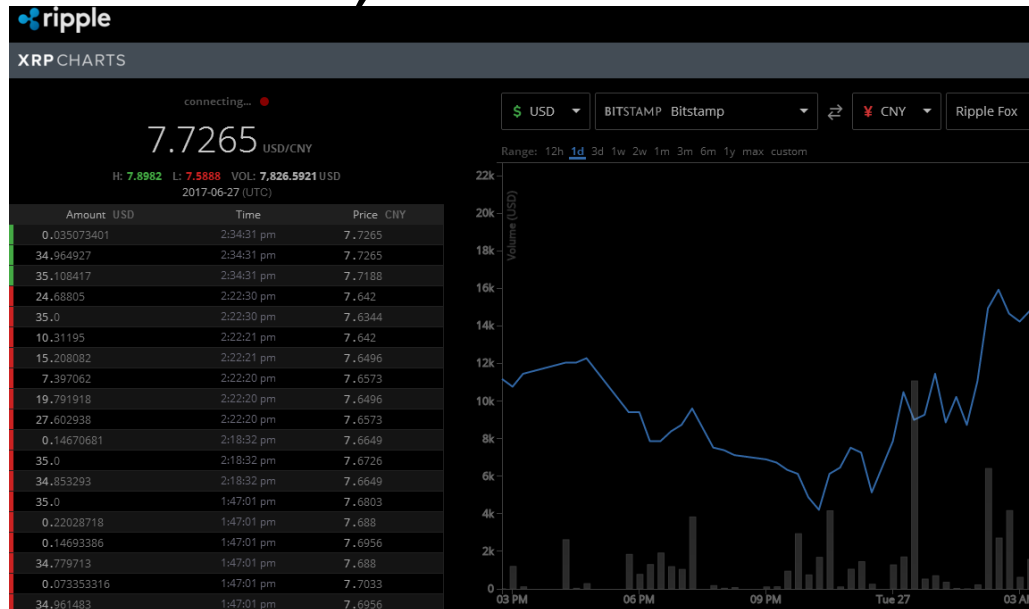
集成合作伙伴



Total 187 validation nodes



USD/CNY on Ripple network as of June 27th, 2017



1 U.S. dollar / Chinese yuan =
6.84251942
Official Rate

Ripple Security (普渡大学的研究)

- A key feature of this network is that when a user has connections to two others, the amounts entrusted to each can vary while the total is kept constant. This creates liquidity: it allows funds to travel, or ripple, around the network. And the user receives a small payment for acting as the intermediary.
- At the end of 2016, the Ripple network consisted of 100,000 wallets and 170,000 credit links. The network has grown considerably—by a factor of 6.6 since 2103 in terms of the number of wallets.
- Some nodes can act like banks by holding real funds and giving the owners credit on the network (and indeed many are banks in the physical world). These are called gateways, and the typical network structure is that wallets connect to gateways (rather than to each other).
- . “Around 50,000 wallets are highly vulnerable to disruption by as few as 10 wallets,” say Moreno-Sanchez and co. “And their credit with the gateways (a total of 14,338,105 USD) is at risk.”

A list of bankrupt gateways

- <https://www.xrpchat.com/topic/3607-a-list-of-bankrupt-gateways-lets-make/>

In the news

Ripple 认为Swift GPI 换汤不换药

After trashing Swift gpi, Ripple hires its biz director

7 hours ago | 1570 views | 0



Ripple has stepped up its rivalry with Swift, poaching the Marjan Delatinne, who had been business director at the messaging network's new gpi programme - an offering Ripple has loudly trashed.

SWIFT and Blockchain

12 January 2017

SWIFT explores blockchain as part of its global payments innovation initiative



22 Banks Join Swift's Cross-Border Blockchain Trial

Jul 6, 2017 at 16:20 by Wolfie Zhao

Blockchain FX Patents

- Goldman Sachs
 - <https://www.google.com/patents/US20160260169>
- Bank of America filing 20+ Blockchain Patents

UTXO security

- ▲index: 索引
- ▲value: 金额
- ▲hash: 一个SHA256的数据摘要
- ▲script: 脚本，这个是重点要讲的

最常用的一个解锁脚本就是P2PKH脚本

```
OP DUP OP HASH160 < Public Key Hash> OP EQUAL
```

解锁时传入签名和公钥组成完整脚本：

```
< Signature> < Public Key> OP DUP OP HASH160 < Public Key
```