OVERVIEW OF BLOCKCHAIN
二次互联网革命？区块链前世今生与未来

WSFC WEBINAR

Julia Zhou周玉琳， CFA, FRM

2016/11

提要：

一.　缘定今生：溯源追本
二　庙堂江湖:私人投资/政府支持
三　君子之国：区块链与支付金融
四.　异曲同工：燎原之势
五　金城汤池？安全与隐忧
六　世界大同？前景与展望

一、河图洛书：溯源追本

二次互联网革命?

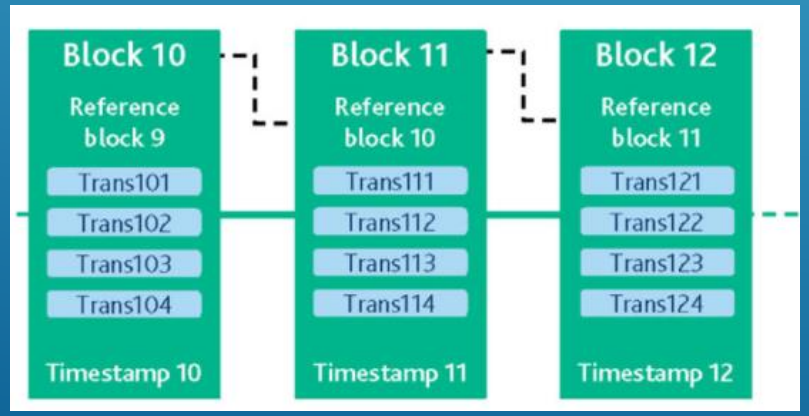
区块链正在给价值的交换形式带来革命性的变化，就像互联网给信息交换和通信带来的革命性变化一样

Blockchain is revolutionising the exchange of value in a similar way to how the internet revolutionised the exchange of information and communication."

-巴克莱银行Barclays

什么是区块链?

- 区块链（blockchain）是一种分布式数据库（distributed database）技术，是通过去中心化和去信任的方式集体维护一个可靠数据的技术方案。
- 每个区块都有一个时间印记并且和前一个区块相连。区块链所有的数据基本都是永久性的，不可更改。它主要的特点在于安全、公开、加密和高效和透明，能够在互不认识或互不信任的多方网络中建立一个可靠的账簿（Ledger），就像它支持比特币（bitcoin)一样。
- 身世成谜: 中本聪（Satoshi Nakamoto）



Picture from: Moody's

六宫粉黛无颜色：落雁沉鱼

区块链魅力:

- 安全性（不可更改，防欺诈防篡改tamper-proof，因为每个区块包括前面区块的信息，并且有哈希加密）
- 公开透明（共识，必须网络里多数节点认同这个数据，才能被加到区块链）
- 加密（非对称式加密）
- 高效（多方共享一个超级账本，虽需多个节点保存但没有对账的麻烦）

技术实现特点:

- 区块、链和时间戳（Block, Chain, and Timestamp
- 分布式结构 (Distributed Ledger Technology, DLT)
- 非对称加密 (Asymmetric Cryptography)

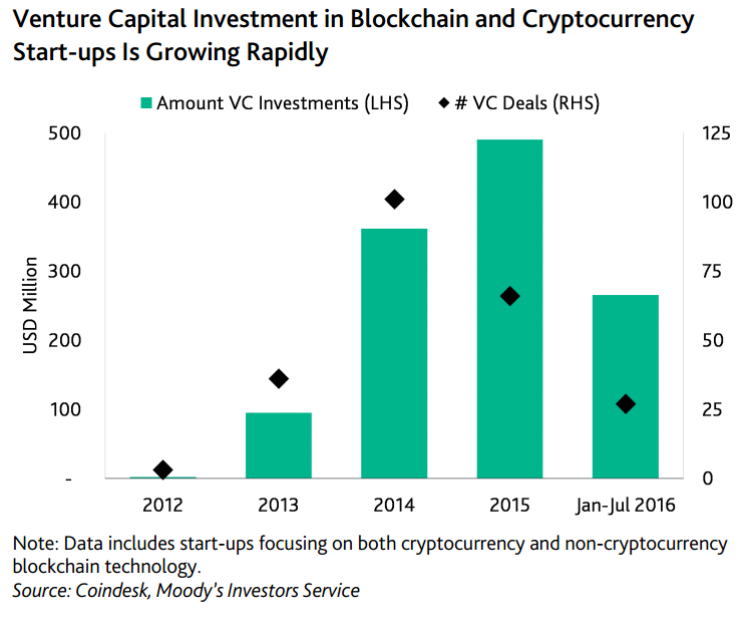
一日看尽长安花：春风得意

- 完全公开链（比特币）
- 联盟链或杂交链 （Ripple）
- 私链或获准进入链 （R3 CEV，Digital Asset, SWIFT's own solution）

二、庙堂江湖:私人投资/政府支持

五陵年少争缠头：私人投资

- 到2016年7月为止，149家专注于加密货币或区块链（blockchain）的初创公司募集了12亿美元投资。
- 区块链逐渐比加密货币本身还更受青睐，2016年Q1，区块链相关的初创公司比加密货币募集到的资金多四倍。
- 传统银行投资：摩根大通2015年在技术投资上已经花了90亿美元，一大重点就是区块链。



Companies	As of 2016/06
Circle	$136亿
Ripple	$0.93亿

Picture from: Moody's

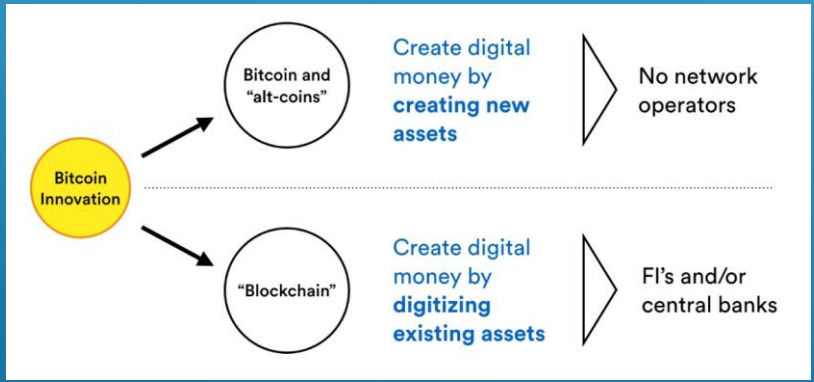
忽复乘舟梦日边：政府支持

- 英国沙盒项目 Sand box
- 新加波 沙盒项目
- 各国央行
- 中国的blockchain尝试 (数字货币）
- 中国招商银行、平安银行和中国外汇交易中心也加入了R3联盟。

三、君子之国：区块链与支付金融

万变其宗：区块链支付本质

- 金融的本质：信任
- 去媒介话
- 任何可以数码化的资产



Picture from: Chain

运用场景

- 天涯比邻：国际支付 （Ripple, Visa): 每年300万亿美元，2000亿美元营收
- 一诺千金：贸易金融：每年230亿美元营收
- 海内一统：银行间超级账本 （R3)
- 化繁为简：资本市场 (Nasdaq, Overstock)
- 天下大同：个人支付 （Circle)
- 后起之秀：保险行业 (B3i)
- 千里鹅毛：商家货币 (Gyft)
- 商鞅变法：央行货币

Picture from: Chain

四、异曲同工：燎原之势

- 地契、房屋证的记录公证
- 学位证书公证
- 客户身份验证Know Your Customer(KYC)/反洗钱Anti-Money Laundering (AML)
- 网络和物联网
- 媒体
- 供应链和物流
- 租车卖车
- 珠宝交易
- 商品验证
- 医疗
- 共享经济
- 选举
- 研究分析和预测领域
- 电力分散供给
- 云计算

五、金城汤池？安全与隐忧

- 北斗南面：51%攻击
- 穷尽数理：密码学破解
- 放之四海：抗压能力
- 偷窃有理？黑客攻击
- 无法无天：法律与监管
- 熊掌与鱼：公链私链

六、世界大同？前景与展望

（一）、蓬山万重

- 高速处理海量交易（比特币弱点）
- 储存海量数据的能力（比特币弱点）
- 跨界跨国的标准化
- 如何更改偶尔失误的错误交易（需要所有参与者有一个都认可的更改机制）
- 大规模化后的运营成本
- 保护商业敏感信息（尤其是银行）
- 没有测试过的大规模全球多领域的共识系统
- 如何实现杠杆金融
- 虚拟货币的波动性
- 环境成本（计算所耗的大量电力

（二）、时不我待

- 区块链初创公司
- 传统金融机构
- 消费者

（三）、星汉灿烂

日月之行，若出其中，星汉灿烂，若出其里