Node 区块链加速器

区块链与创新创业

http://www.node.ac

李晋

西安电子科技大学 通识课程 2021春季学期

Node 区块链加速器

PART 5
可编程货币、通证经济与分布式数字金融

Node 区块链加速器

5.1
可编程货币

可编程货币

- （以区块链技术为底层），具备分布式共识的加密数字货币，可以用运行于其上的智能合约程序代码，直接实现交易逻辑，而非依赖于货币本身之外的系统完成交易

Node 区块链加速器

5.2
通证与通证经济

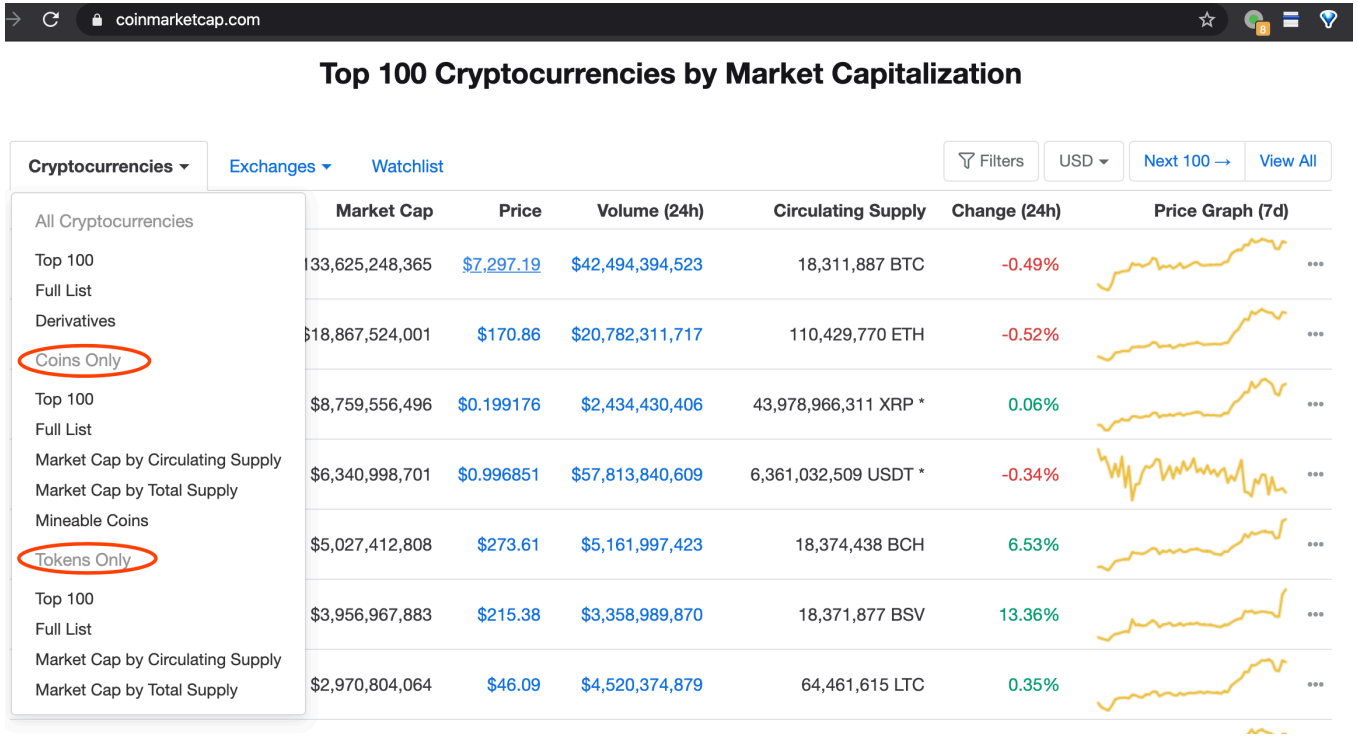
一 通证是什么

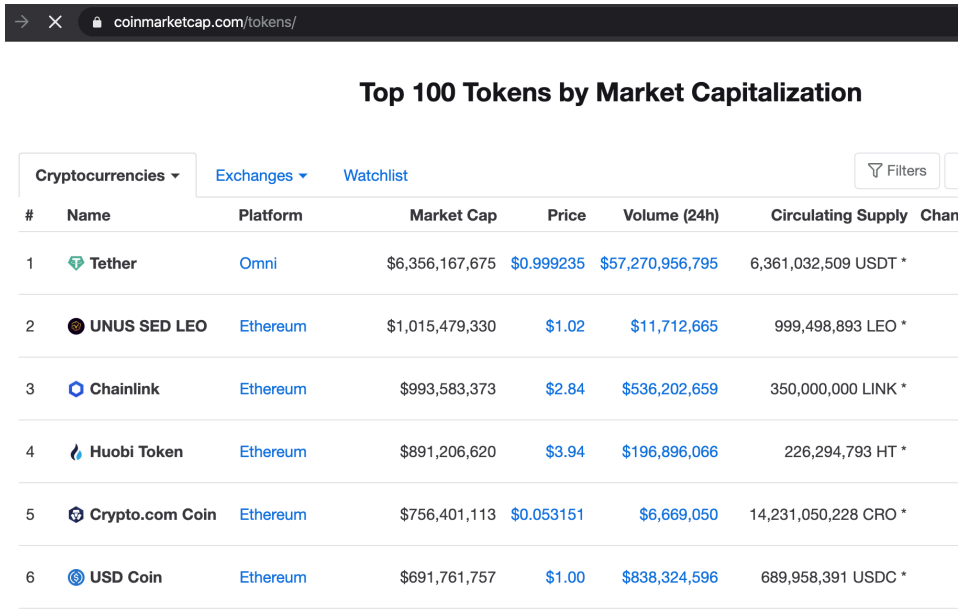
- token释义： 表征；代币；记号；令牌；凭证；通证
- 是一种可流通的数字凭证，权益证明
- 最早翻译为“代币”，后来孟岩提出“通证”，现已被广泛接受

Node 区块链加速器

通证与加密数字货币

- 早期区分：
  - 原生币coin：区块链底层币（一阶币）
  - 代币token：区块链上层使用智能合约创建的币





一 通证与加密数字货币

- 狭义 token 单指用智能合约生成的 token
- 广义 token 的概念囊括了 coin 和狭义 token
- coin 与 token 在项目不同阶段会转化（例：EOS）
- 界限逐渐模糊，其涵义逐渐由其功能性而非技术性区分

通证的好处

- 发行门槛低
- 流通性强
- 操作灵活

Node
区块链加速器

用智能合约发行token的好处

- 成本：发行token不需要自己搭链并形成分布式共识，只需要基于已经成熟的链，编写（或copy）上层代码即可发行
- 灵活性：抽象层次高，上层代码灵活性使得对token的操作可以附加很多功能，成为可编程数字金融的基础

以太坊的token规范

- 常见的token规范如： ERC20（同质化代币）、ERC721（非同质化代币）、ERC1400（证券型代币）
- ERC： Ethereum Request for Comment（类似RFC），由EIP而来，经过批准后确定

Accepted

Number	Title	Author
1057	ProgPoW, a Programmatic Proof-of-Work	IfDefElse, Greg Colvin

Final

Number	Title	Author
2	Homestead Hard-fork Changes	Vitalik Buterin
6	Renaming SUICIDE opcode	Hudson Jameson
7	DELEGATECALL	Vitalik Buterin
8	devp2p Forward Compatibility Requirements for Homestead	Felix Lange
20	ERC-20 Token Standard	Fabian Vogelsteller, Vitalik Buterin
55	Mixed-case checksum address encoding	Vitalik Buterin, Alex Van de Sande
100	Change difficulty adjustment to target mean block time including uncles	Vitalik Buterin

以太坊的token规范

- 相当于软件程序接口规范，不是代码实现
- 例：ERC20的接口
  - **totalSupply()**：
    返回代币供给总量
  - **balanceOf(address _owner)**：
    返回_owner的帐户余额
  - **transfer(address _to,uint256 _value)**：
    并将数量为_value的代币转入地址_to并触发transfer事件
  - **transferFrom(address _from,address _to,uint256_value)**：
    将地址_from中的_value数量的代币转入地址_to ， 并触发transfer事件
  - **approve(address _spender,uint256 _value)**：
    允许_spender提取限额_value的代币
  - **allowance(address _owner,address _spender)** ：
    返回_spender可从_owner提款的代币数量上限
- 提醒：代码实现中的安全漏洞，是很大挑战，甚至导致项目直接失败

token规范的好处

- 互操作性
- 共用基础设施（钱包、浏览器、交易所等）
- 从而使创建token的成本更低

一 通证的价值和意义

- 商业计量的媒介
- 凭证、权益证明
- 支付媒介
- 价值存储
- 激励手段：通过通证符号，让一个经济系统的利益相关方，激发其更高的参与度。即通过生产关系的优化，提高生产效率。

通证与区块链的关系

- 通证不是必须的：一些场景可以采用“无币区块链”
- 通证不一定基于区块链技术
- 区块链 + 通证，是最佳组合：
  - 发行机制透明，更容易达成可信共识
  - 流动性更强

一 通证经济的发展现状

- 早期的币圈、链圈之分
- 炒币、投机、非法诈骗，造成负面解读，“币”也易引起敏感
- 至今已经基本形成融合，无法硬性割裂
- “它就像幽灵，人人都知道，但却没有人见过”
- 难点：纯币圈的人不在乎所谓通证经济，而链圈的人偏技术，没有真正理解通证，更无能力设计通证系统

通证的分类

- 瑞士金融市场监督管理局（FINMA）2018.2区分：
  - 支付型代币 Payment token
  - 功能型代币 Utility token
  - 资产型代币 Asset token
- 美国证券交易委员（SEC）：
  - 实用型通证 Utility token
  - 证券型通证 Security token

Node 区块链加速器

5.3
通证系统设计

通证系统的设计目标

- 如何让参与系统的利益相关方，通过通证的方法有效激励，使各方更好的协作与交换，进而创建可持续发展的业务

Node
区块链加速器

通证系统的设计要点

- 围绕通证的产生、分配、交易，主要有两方面：
  - 激励机制：如何达到使用token产生激励效果？
  - 治理结构：组织和系统如何透明、高效、合法的管理、监督，确保各方利益有保障？

Node 区块链加速器

5.4
分布式数字金融

Node 区块链加速器

ICO的创新与泡沫

ICO（Initial Coin Offering）

- 用加密货币进行公开募资，通过发行、出售token，募集比特币、以太坊等主流加密货币
- 俗称“发币”
- 常见流程：项目白皮书 -> 发行token -> 公开市场认购（募资） -> token上交易所，持有者可自由交易
- 由于比特币、以太坊不被法律认为是货币，所以绕开了公募监管
- 后来又出现了IFO、IEO等玩法

ICO（Initial Coin Offering）

- 2013年出现，高峰是2017年中
- token大多数是utility token，对某种服务的使用权，但这种服务是否真有价值不好说
- 2017.9.4，七部委联合发布《关于防范代币发行融资风险的公告》，指出：代币发行融资本质上是一种未经批准非法公开融资的行为。但并未止住势头，转战海外
- 空气，真假难辨，击鼓传花，疯狂犹如2000年的互联网，“三点钟无眠区块链”
- “全球人民的财富转移游戏”，零和性
- 2017年底，传统资本入场
- 2018年上半年，伴随比特币价格暴跌，ICO转冷
- 并非没有创新和价值，但被完全玩坏了

ICO（Initial Coin Offering）

- ICO的创新：
  - 效率。但绕过监管是本末倒置的做法，去中心化的金融环境还完全不成熟
  - 组织变革，彻底挑战了“公司”、“股权”这些传统概念，模糊了投资人、消费者的界限，从中依稀看到了未来全新的社会组织方式（DAC、DAO）
- ICO的缺点：
  - 缺乏法规，极易滋生诈骗，劣币驱逐良币，创新的代价
  - 一次性融到，不符合精益创业原则，资本使用效率极低

DAICO

- V神在2018年1月提出的ICO改进模型
- 设置资金分阶段解锁机制，投资人根据项目进展投票决定是否继续解锁资金，或收回资金
- 用智能合约实现

Node 区块链加速器

Security Token 证券型通证

Security Token 证券型通证

- 证券（Security）：一种财产权的有价凭证，持有者可以依据此凭证，证明其所有权或债权等私权的证明文件
- Unit of Onwership：所有权的单位分割
  - 早期：交易员在黑板上对价格
  - 电话时代：打电话进行撮合交易
  - 现代：电子化交易引擎
- 所有权凭证：纸质stock certificate->电子化eshares -> 区块链Token

Node 区块链加速器

如何区分通证是不是证券型Token？

- Howey Test

"a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party. "

STO（Security Token Offering）

- 证券化：把某种财产权的现金流收益打包，卖给第三方投资者的过程
- 法律对证券的监管通常极为严格
- STO：与传统的证券化过程没有本质差异，但使用了加密货币作为载体。受原有法律监管。与ICO有本质差别

STO（Security Token Offering）

- 案例：
  - Telegram：通过非公开销售GRAM token，融资17亿美金
  - EOS：融资42亿美金，证券属性较为明显，争议巨大

Node 区块链加速器

数字货币交易所

Node 区块链加速器

稳定币

通证举例：稳定币

- 稳定币（Stable Coins）：以法币价格衡量，价格相对稳定的加密货币
- 作用：
  - 法币桥梁
  - 资金避险
  - 资产储值
  - 支付结算
  - 交易对

通证举例：稳定币

- 案例1：USDT，采用中心化资产抵押
  - Tether公司发行，背后是香港BitFinex交易所
  - 以相同面额的USD作为准备金存储于银行，可随时兑换，实现锚定，类似曾经美元与黄金挂钩
  - 将链上资产与链下资产映射打通
  - 已发行量$30亿美金
  - 优：简单高效，流动性好
  - 劣：依赖中心化审计监管，存在超发可能，信用风险
  - 最早使用OmniLayer协议，构建于比特币之上的代币。后来发行了基于ERC20的代币

通证举例：稳定币

- USDT的挑战者： TrueUSD、USDC、 GUSD、PAX等
- 其中USDC由Circle和Coinbase推出，后两者由NYDFS（纽约金融服务部）批准

通证举例：稳定币

- 案例2：BitCNY、BitUSD，采用去中心化资产抵押
  - 通过抵押去中心化的资产来创造稳定币，抵押资产被存放于智能合约中，不必依赖第三方审计监管
  - 资产均为链上资产
  - 优：具备去中心化的优势，抵押资产透明，不受人为操纵
  - 劣：抵押资产本身价格波动大，导致风险控制可能失效；需要超额抵押多于发行的稳定币的资产；实际情况是稳定性不尽人意
  - 使用BitShares作为平台和抵押物
  - 其他如：基于MakerDAO的DAI

通证举例：稳定币

- 案例3：Basis(Basecoin)，基于算法银行

Node 区块链加速器

基于区块链的资产证券化

资产证券化

- 资产证券化是指以资产未来所产生的现金流为偿付支持，进行信用增级，发行资产支持证券（Asset-backed Securities, ABS）的过程
- 本质上就是出售未来权益以进行融资
- 资产证券化现状：认购方数量少，多为信托、银行、保险等国营财团；发售方门槛高、流程手续复杂、审计麻烦；流动性低；法制开放程度低，民间可操作空间窄；中心化登记，操作程序复杂
- 区块链为资产证券化提供了更高效的记账和信息披露方法，提高了效率和可信性，能够大幅激发其活力

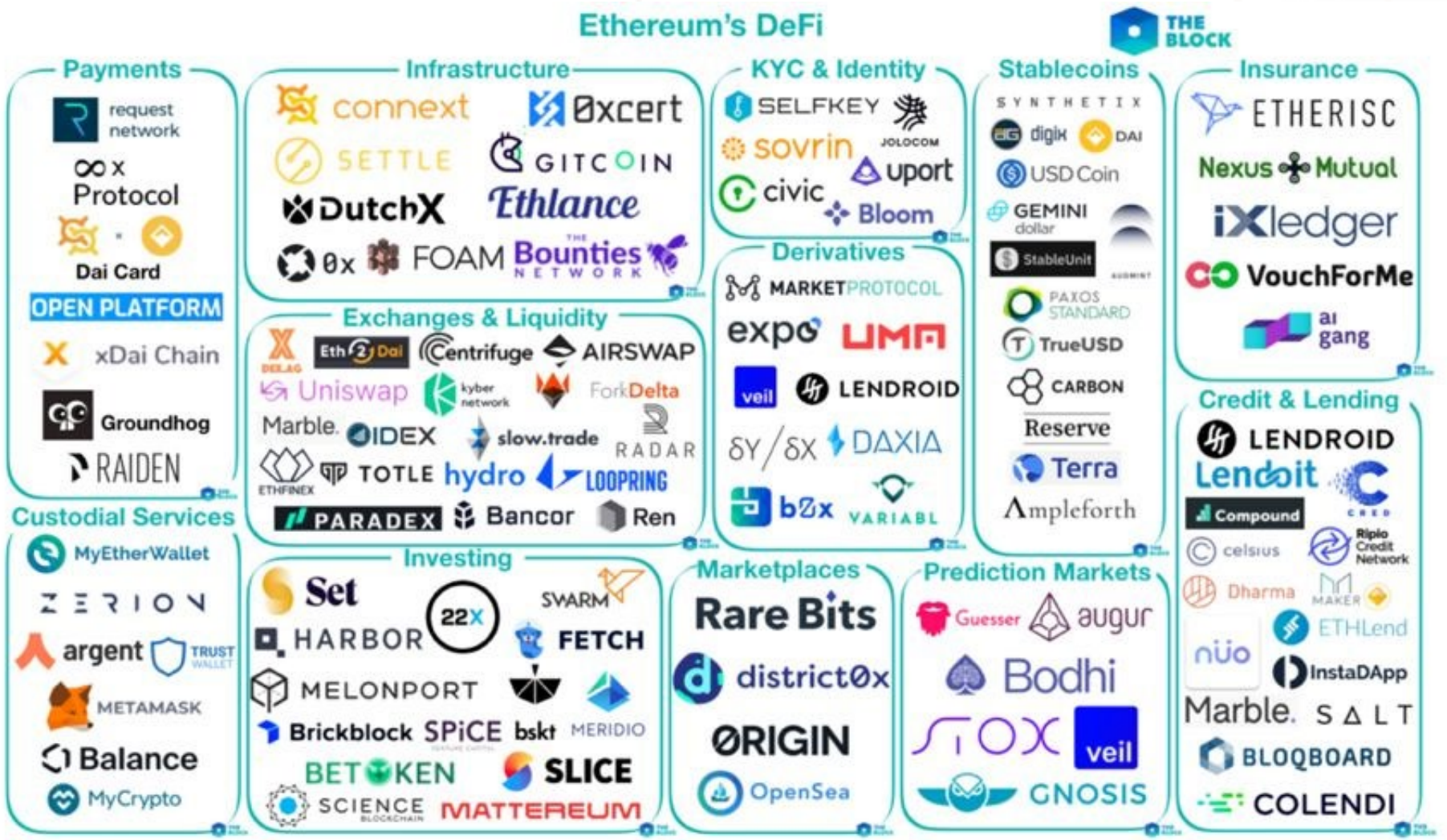
Node 区块链加速器

DeFi：分布式金融初探

DeFi（Decentralized Finance）

- 通过区块链、智能合约实现了去中介化，提供金融效率、降低成本
- 建立在资产通证化基础上
- 无需可信第三方，数据公开透明，智能合约自动交易
- 应用如：稳定币、DEX（去中心化交易所）、借贷、衍生品、预测市场、保险平台等
- 目前处于早期探索期，发展很快，引领近一年的金融热潮
- 案例： MakerDAO、Compound等

以太坊上的DeFi应用



Node 区块链加速器

5.5 法定数字货币：过渡还是终局？

Node 区块链加速器

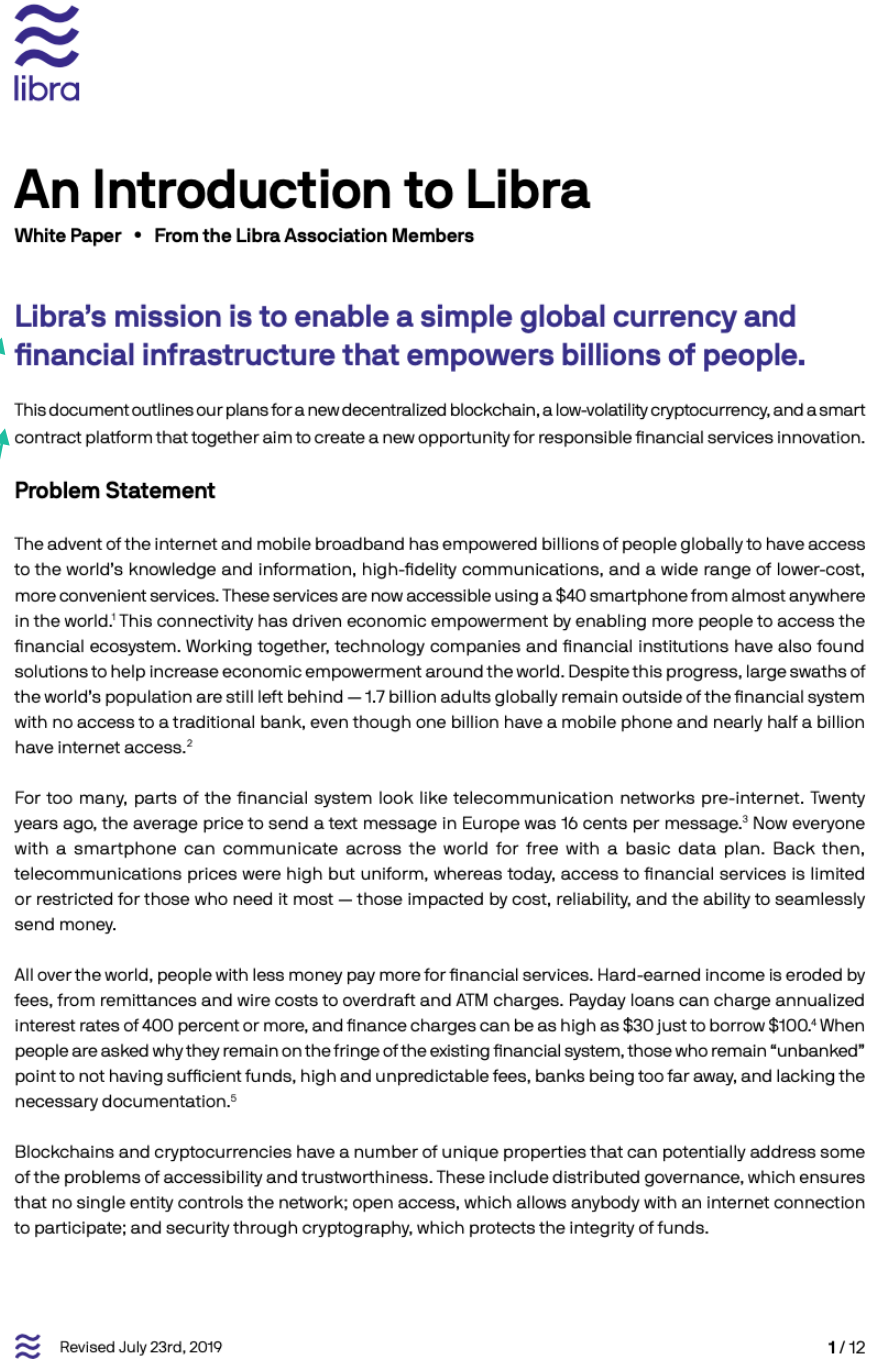
Libra：超主权货币的宏大蓝图

Libra

- 今年6月，Facebook发布Libra白皮书
- 关键词：普惠金融，货币互联网，无国界货币，区块链（许可链），真实资产储备篮子，Libra协会
- 继比特币、以太坊之后的又一里程碑事件

Libra 的使命是建立一套简单的、无国界的货币和为数十亿人服务的金融基础设施。

本白皮书概述了我们努力打造一个新的去中心化区块链、一种低波动性加密货币和一个智能合约平台的计划， 以期为负责任的金融服务创新开创新的机遇。



libra

An Introduction to Libra

White Paper • From the Libra Association Members

Libra's mission is to enable a simple global currency and financial infrastructure that empowers billions of people.

This document outlines our plans for a new decentralized blockchain, a low-volatility cryptocurrency, and a smart contract platform that together aim to create a new opportunity for responsible financial services innovation.

Problem Statement

The advent of the internet and mobile broadband has empowered billions of people globally to have access to the world's knowledge and information, high-fidelity communications, and a wide range of lower-cost, more convenient services. These services are now accessible using a $40 smartphone from almost anywhere in the world.[1] This connectivity has driven economic empowerment by enabling more people to access the financial ecosystem. Working together, technology companies and financial institutions have also found solutions to help increase economic empowerment around the world. Despite this progress, large swaths of the world's population are still left behind — 1.7 billion adults globally remain outside of the financial system with no access to a traditional bank, even though one billion have a mobile phone and nearly half a billion have internet access.[2]

For too many, parts of the financial system look like telecommunication networks pre-internet. Twenty years ago, the average price to send a text message in Europe was 16 cents per message.[3] Now everyone with a smartphone can communicate across the world for free with a basic data plan. Back then, telecommunications prices were high but uniform, whereas today, access to financial services is limited or restricted for those who need it most — those impacted by cost, reliability, and the ability to seamlessly send money.

All over the world, people with less money pay more for financial services. Hard-earned income is eroded by fees, from remittances and wire costs to overdraft and ATM charges. Payday loans can charge annualized interest rates of 400 percent or more, and finance charges can be as high as $30 just to borrow $100.[4] When people are asked why they remain on the fringe of the existing financial system, those who remain "unbanked" point to not having sufficient funds, high and unpredictable fees, banks being too far away, and lacking the necessary documentation.[5]

Blockchains and cryptocurrencies have a number of unique properties that can potentially address some of the problems of accessibility and trustworthiness. These include distributed governance, which ensures that no single entity controls the network; open access, which allows anybody with an internet connection to participate; and security through cryptography, which protects the integrity of funds.

Revised July 23rd, 2019

1 / 12

Node 区块链加速器

DC/EP：中国的法定数字货币

DC/EP推出的大背景

- 中央使用金融工具调控力度加大
- 人民币国际化
- 一带一路
- 中美之争
- 保护自己的货币主权和法币地位

DC/EP的历史和意义

- 中国人民银行正在全速推进法定数字货币
- 央行数字货币研究所，已有几年的研发时间，早于Libra
- Libra的推出，加速了DCEP的速度：
  - Libra目标是覆盖全球。从支付结算，渗透到储蓄、投融资、保险、资产交易等每个领域。直接替代了银行
  - Libra的储备金中，美元占绝对大比例
  - 超主权货币会挤压人民币的空间。如果人民币未能纳入全球化金融体系，地位肯定会削弱

DC/EP的特点

- M0货币，现钞替代物，与银行支付、支付宝、微信支付不同（M1：狭义货币，M2：广义货币）
- 法偿性，刚性兑付
- 保持现钞的属性和主要特征，便于携带，交易可匿名

DC/EP的意义

- 作为国际贸易结算货币，降低使用门槛，提升使用效率和体验，有助于人民币国际化
- 加强中央对金融的管控
- 对第三方支付平台的削弱
- 不仅仅是数字化钞票，对传统金融体系将有巨大冲击
- （不一定基于区块链技术）

DC/EP的推进情况

- 国字号4大行（中、工、农、建）+交行、邮储，及3大运营商为主参与建设
- 最初在深圳、苏州试点，2019年底，在小范围封闭试点，如公交支付
- 目前已在全国多个城市大范围试点

Node 区块链加速器

课后作业

课后作业

1. 构思并简要设计一个带有通证体系的系统，如通证版的 Wikipedia 或 GitHub

Node 区块链加速器

扩展阅读

参考资料（本次课）

https://github.com/ethereum/EIPs

https://eips.ethereum.org/all

Tether: Fiat currencies on the Bitcoin blockchain（Tether白皮书：一种利用比特币区块链交易的法币代币）

孟岩：参与设计20多个区块链经济系统后，我总结出4个原则和7个陷阱
https://zhuanlan.zhihu.com/p/35389431

全球区块链政策监管趋势研究：对ICO项目的五种态度
https://36kr.com/p/5137250.html

Libra白皮书

比特币的十年历史
http://8btc.com/thread-240704-1-1.html

Node 区块链加速器

课程总结

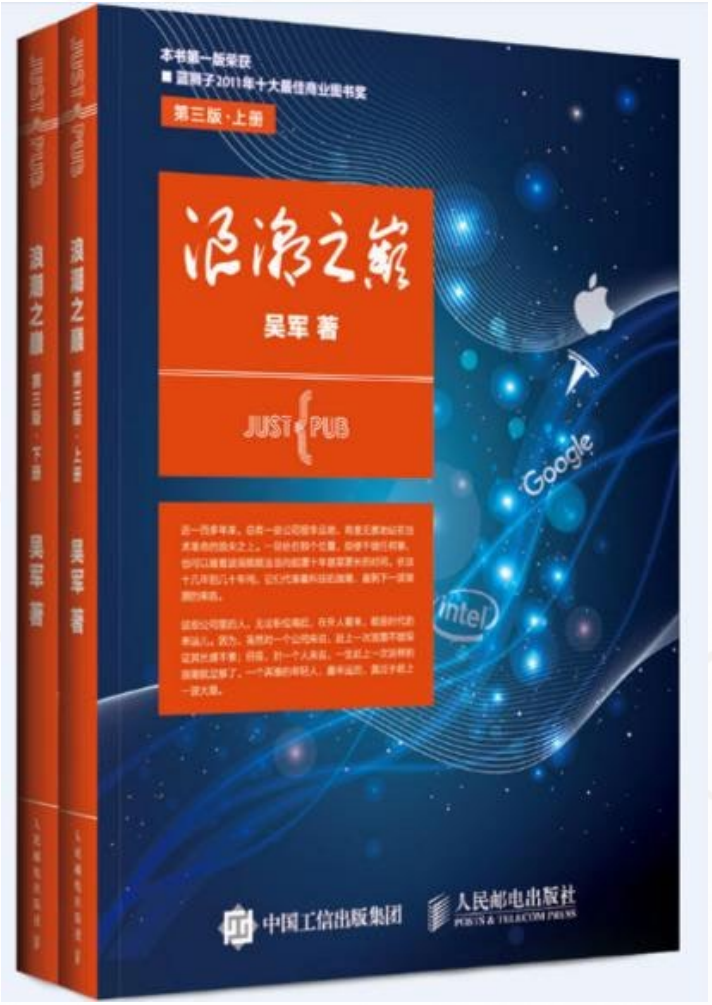
> 一篇天才短文，开创崭新世界。十年不短，无出其右；十年不长，激荡其后。十年来，有人炒币、霸矿、山寨造链，有人布道、学习、砥砺创新。十年后，期待发宏愿之士、大智慧之作。

— 李军，清华大学教授，2018

比特币的10年历史

近一百多年来，总有一些公司很幸运地、有意识或者无意识地站在技术革命的浪尖之上。一旦处在了那个位置，即使不做任何事，也可以随着波浪顺顺当当地向前漂个十年甚至更长的时间。在这十几年间，它们代表着科技的浪潮，直到下一波浪潮的来临。

这些公司里的人，无论职位高低，在外人看来，都是时代的幸运儿。因为，虽然对一个公司来说，赶上一次浪潮不能保证其长盛不衰；但是，对一个人来说，一生赶上一次这样的浪潮就足够了。一个弄潮的年轻人，最幸运的，莫过于赶上一波大潮。



— 吴军《浪潮之巅》

> The best way to predict the future is to invent it!
>
> 预测未来的最好方式就是去创造它!

— Alan Kay, 1971