QCon 全球软件开发大会
INTERNATIONAL SOFTWARE
DEVELOPMENT CONFERENCE

BEIJING 2018

《代币经济学的工程设计》

演讲者 / Michael Yuan 博士

主办方 Geekbang> 极客邦科技 InfoQ

GTLC
GLOBAL
TECH LEADERSHIP
CONFERENCE

全球技术领导力峰会

通往**年薪百万**的CTO的路上，

如何打造自己的技术**领导**力？

扫描二维码了解详情

www.CyberMiles.io

CyberMiles

SIG
SUSQUEHANNA

BUILDING BLOCKCHAIN APPS

MICHAEL YUAN

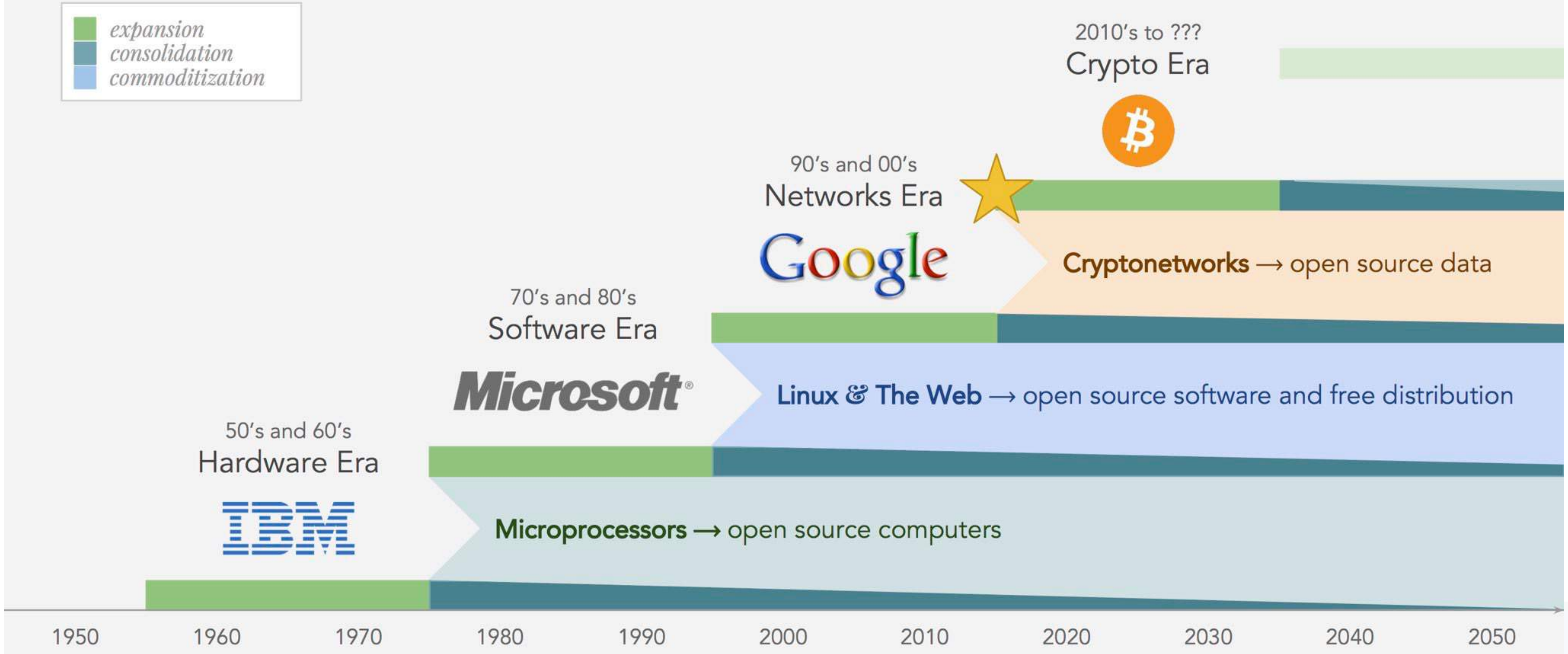
Disclaimer

This presentation contains forward-looking statements that are based on the beliefs of Cybermiles Foundation Limited (“CyberMiles”), a company limited by guarantee incorporated in Hong Kong, as well as certain assumptions made by and information available to CyberMiles. No representation or warranty is given as to the achievement or reasonableness of any plans, future projections or prospects. If and when the CyberMiles platform is completed, it may differ significantly from the one set out in this document.

Furthermore, no representations or warranties are made as to the accuracy or completeness of the information, statements, opinions or other matters described in this presentation or otherwise communicated. Nothing in this presentation is or should be relied upon as a promise or representation as to the future or investment advice. To the fullest extent permitted under applicable law, all liability for any loss or damage whatsoever (whether foreseeable or not) arising from or in connection with any person acting on this presentation, or any aspect of it, notwithstanding any negligence, default or lack of care, is disclaimed. To the extent liability may be restricted but not fully disclaimed, it is restricted to the maximum extent permitted by applicable law.

The views and opinions expressed in this paper are those of the CyberMiles only. They are not advice, nor an offer or solicitation of any kind, nor may they be relied upon for any purpose. CMT and the CyberMiles platform are not intended to constitute securities or any other regulated products in any jurisdiction. Please obtain any necessary professional advice.

Open Standards and Investment Returns



🟩 *expansion*
🟦 *consolidation*
🟦 *commoditization*

50's and 60's
Hardware Era

70's and 80's
Software Era

90's and 00's
Networks Era

2010's to ???
Crypto Era

Microprocessors ⟶ open source computers

Linux & The Web ⟶ open source software and free distribution

Cryptonetworks ⟶ open source data

中本聪最重要的贡献

Cryptoeconomics 加密（代币）经济学

区块链的杀手级应用

- 数字黄金
- 代币发行

It’s important to remember that if there were no Bitcoin, there would be no distributed ledger technology.
-- Christopher Giancarlo, CFTC Chairman, 2018

Capital formation is going to be the main app of blockchain.
-- David Sacks, 2018

代币是什么？

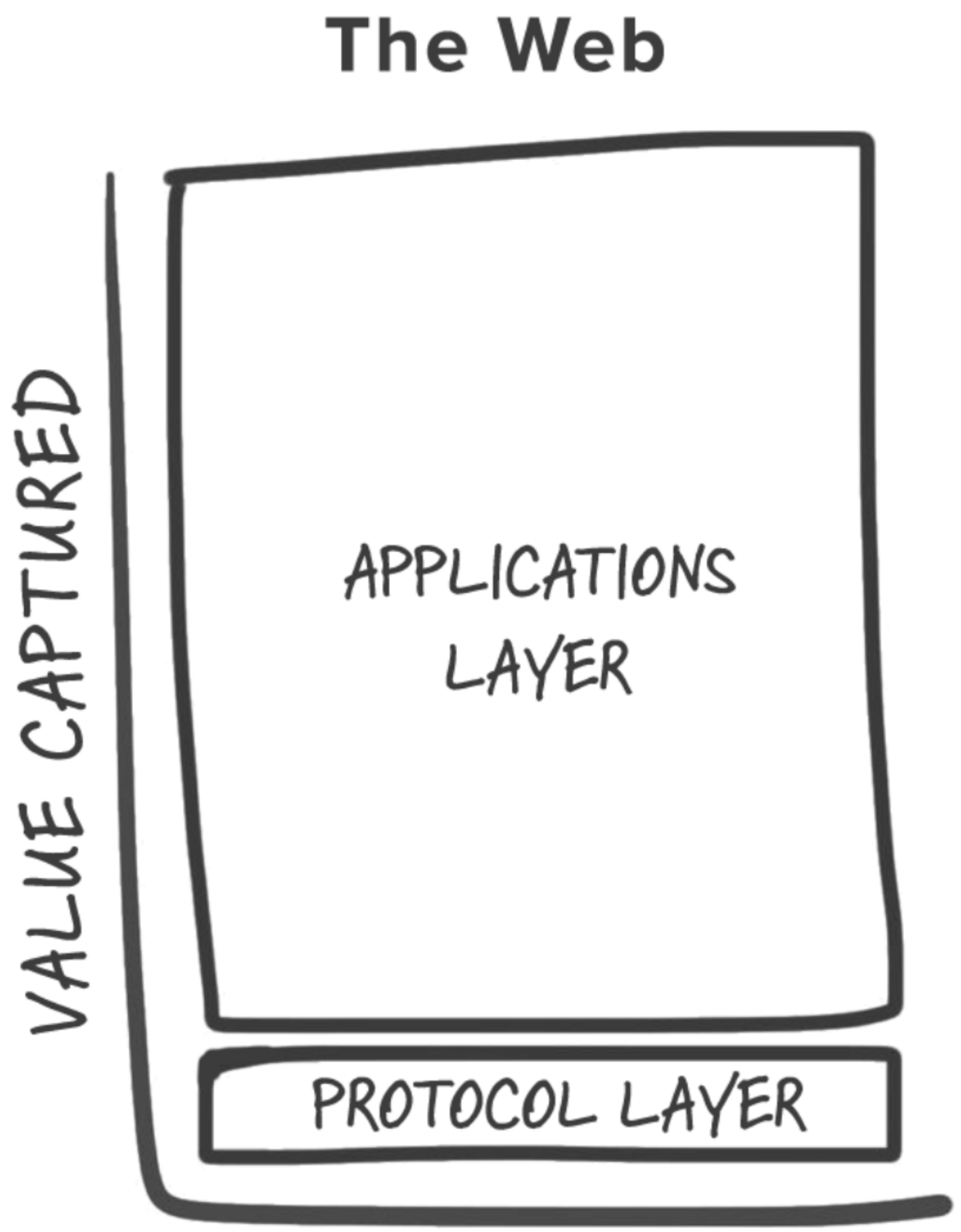
- 网络代币：保证区块链网络正常运行的机制
  - 安全（BTC，ETH）
  - 高性能（DPoS 质押币, CMT）
- 应用代币：商业应用的激励机制
  - FileCoin, App Coins
- 证券代币
  - 智能化高流通性的股权
  - 智能化的使用权

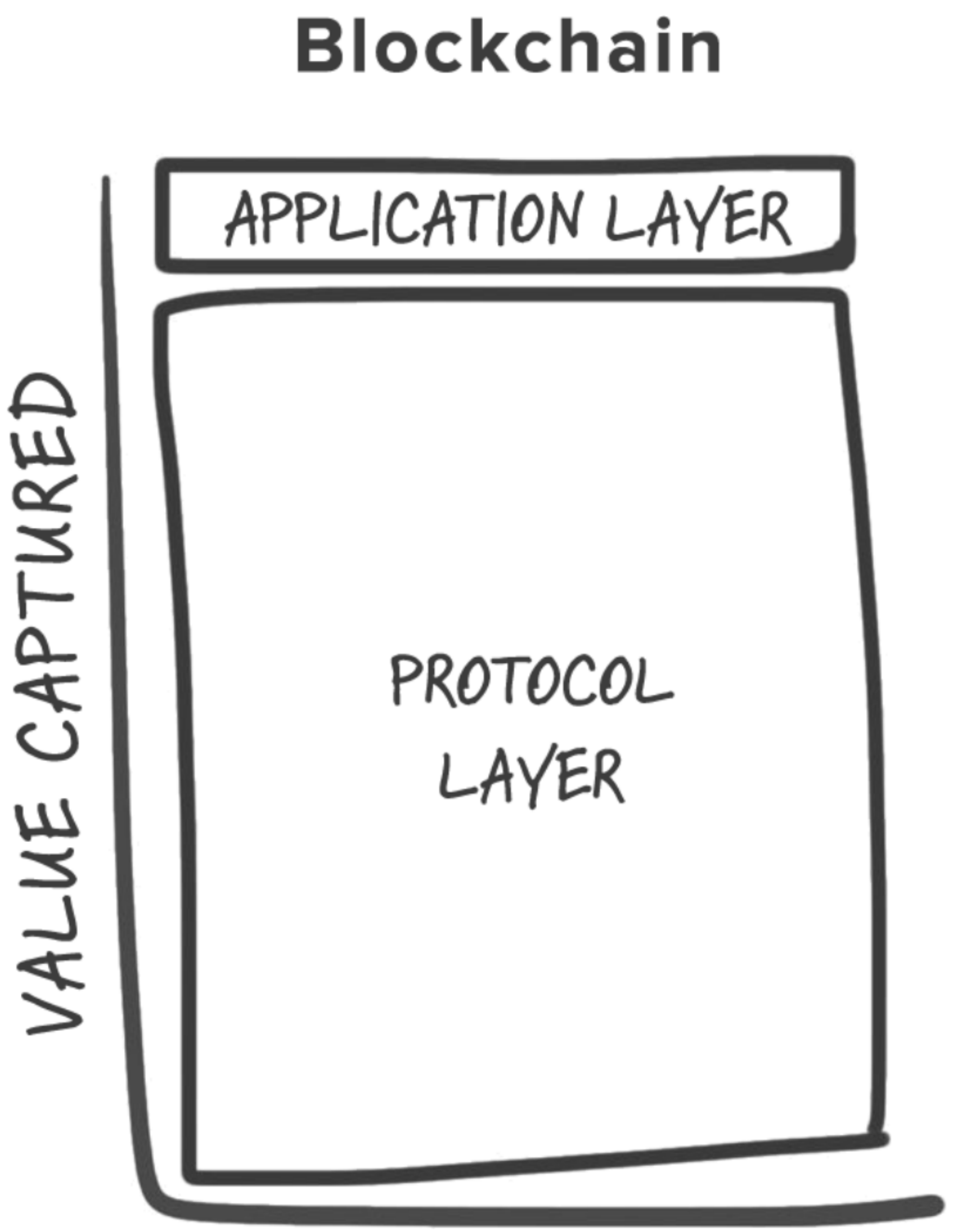
代币的实现

- ERC 20
- ERC 223
- ERC 721
- ERC 884
- ERC 867 (fund recovery)

网络代币

重协议，轻应用


The Web
VALUE CAPTURED
APPLICATIONS LAYER
PROTOCOL LAYER


Blockchain
VALUE CAPTURED
APPLICATION LAYER
PROTOCOL LAYER

区块链应用的瓶颈

- 性能差
- 负网络效应
- 安全性差
- 开发非常困难

用经济机制设计解决技术问题

- 性能问题：新的共识机制
- 可扩展性问题：侧链与跨链资产交换机制
- 安全性问题：惩罚攻击者的治理机制
- 易用性问题：用通胀取代交易费

CyberMiles 的实践经验

加入我们的测试链，Travis

www.CyberMiles.io

性能问题

- 经济机制
  - DPoS 共识机制
  - 全兼容以太坊，但是比以太坊块 100 倍
- 软件工程
  - 系统性地重用数字签名
  - 虚拟机的大量改进，包括新的编程语言 Lity
  - 高并发的 transaction pools

DPoS 的经济机制

- 为什么要质押代币？
  - 安全的来源是作恶惩罚的机制
  - 获得：获得回报（通胀的一部分）
  - 付出：交易流动性，可能的作恶惩罚
- 质押代币对经济的影响
- 如何防止寡头？
- 贿选的问题
  - 利益分配的公开透明化

可扩展性问题

- 侧链与二级网络
  - Lightning, Plasma and Raiden
  - 用链上资产保证侧链交易的合法性
- 跨链
  - Cosmos, Polkadot
  - 跨链资产的证明与销毁
- 软件工程
  - Sharding

安全问题

- 经济机制
  - EIP 867
  - 链上透明的决策机制，由见证人投票决定回滚攻击的交易
- 软件工程
  - 在协议层上预防高风险交易
  - 安全的开发工具

易用性问题

- 经济机制
  - 大部分交易不收交易费
  - SPAM 与重度用户需要付交易费
  - 见证人通过通胀获利
- 软件工程
  - 新的虚拟机编程语言 Lity

什么是 Lity

- CyberMiles 的虚拟机编程语言
- 全兼容 Solidity
- 提供 Native Interface 大幅提高性能
- 语法支持规则引擎 (rules engine)
- 语法支持商业流程 (business processes)
  - 支持长期商业合约

应用代币

公司与网络

- Theory of the firm: 降低生产的交易成本
  - 工业时代的 vertical integration 与规模效应
- 互联网巨头都是网络的建设者
  - 互联网的本质是网络效应
  - 公司建立，运营网络；制订规则，保证规则的执行；冷启动网络
  - 但是在网络正常运营之后，公司主要就是寻租
- 区块链本身就是网络
- 区块链世界股权价值很低

应用层的协议

Internet of Blockchains!

货币的必要条件

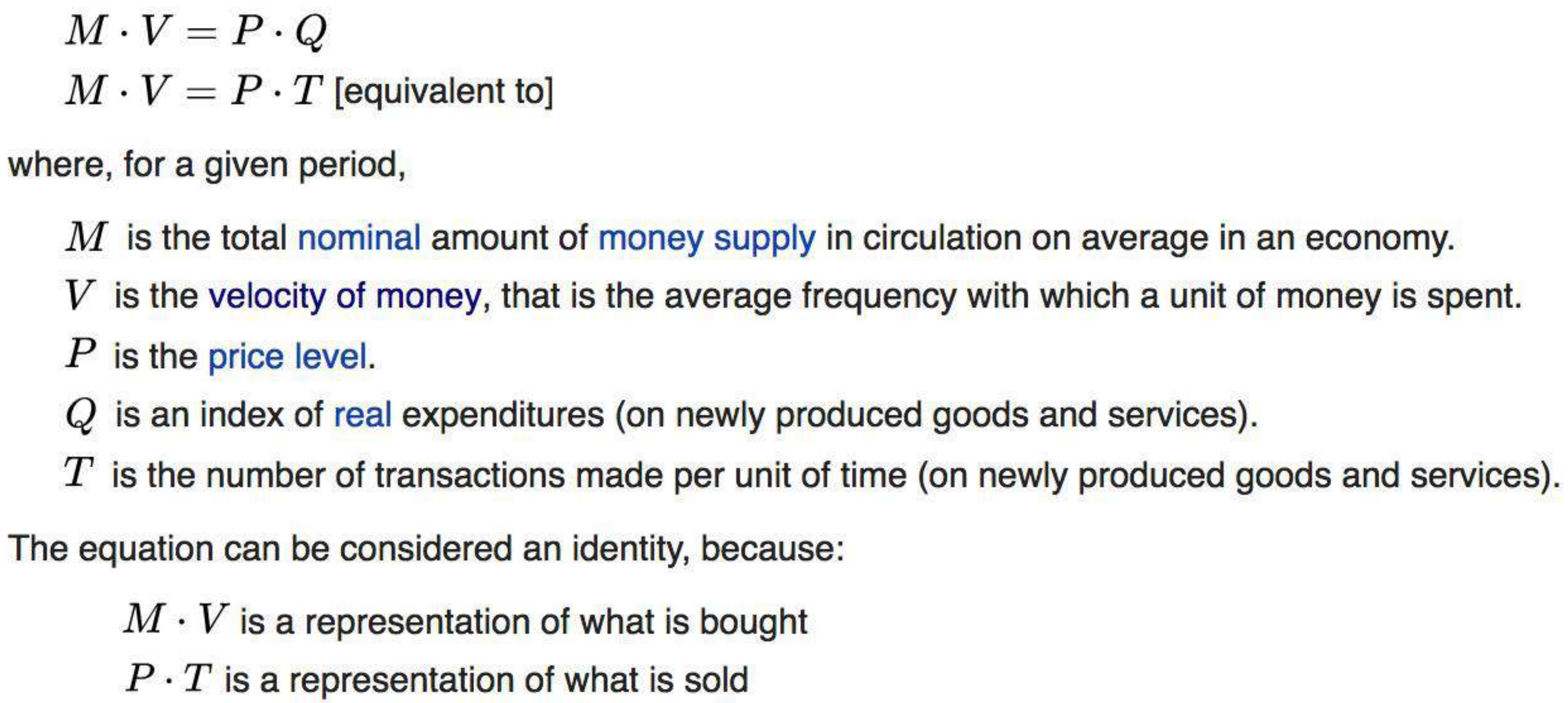
- 交易的中介
- 价值的体现

To be successful, money must be both a medium of exchange and a reasonably stable store of value.
-- Paul Krugman, Nobel Laurate, in “Bitcoin is Evil”, 2013

代币机制设计的关键

- 不可替代的交易属性
- 低流动性

代币的内在价值



$$M \cdot V = P \cdot Q$$

$$M \cdot V = P \cdot T \text{ [equivalent to]}$$

where, for a given period,

M is the total nominal amount of money supply in circulation on average in an economy.

V is the velocity of money, that is the average frequency with which a unit of money is spent.

P is the price level.

Q is an index of real expenditures (on newly produced goods and services).

T is the number of transactions made per unit of time (on newly produced goods and services).

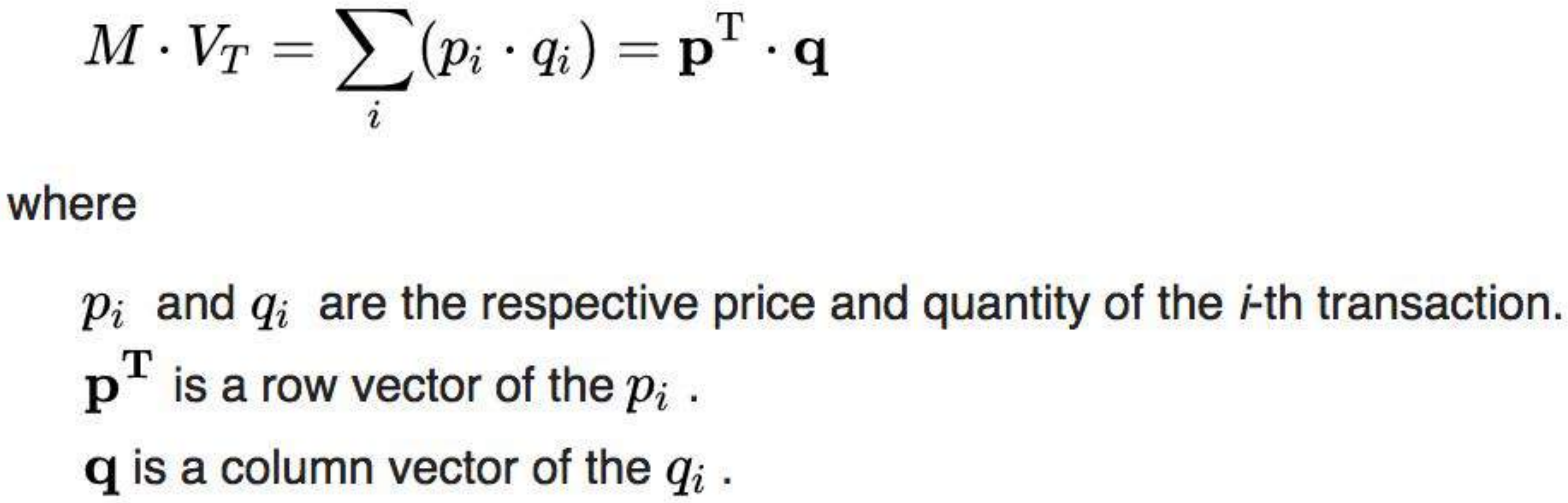
The equation can be considered an identity, because:

$M \cdot V$ is a representation of what is bought

$P \cdot T$ is a representation of what is sold

$$Present\ Value\ of\ Monetary\ base = M = \frac{P \cdot Q \cdot (1 + gr\%)^n}{V \cdot (1 + dr\%)^n}$$

代币的内在价值



$$M \cdot V_T = \sum_i (p_i \cdot q_i) = \mathbf{p}^{\mathrm{T}} \cdot \mathbf{q}$$

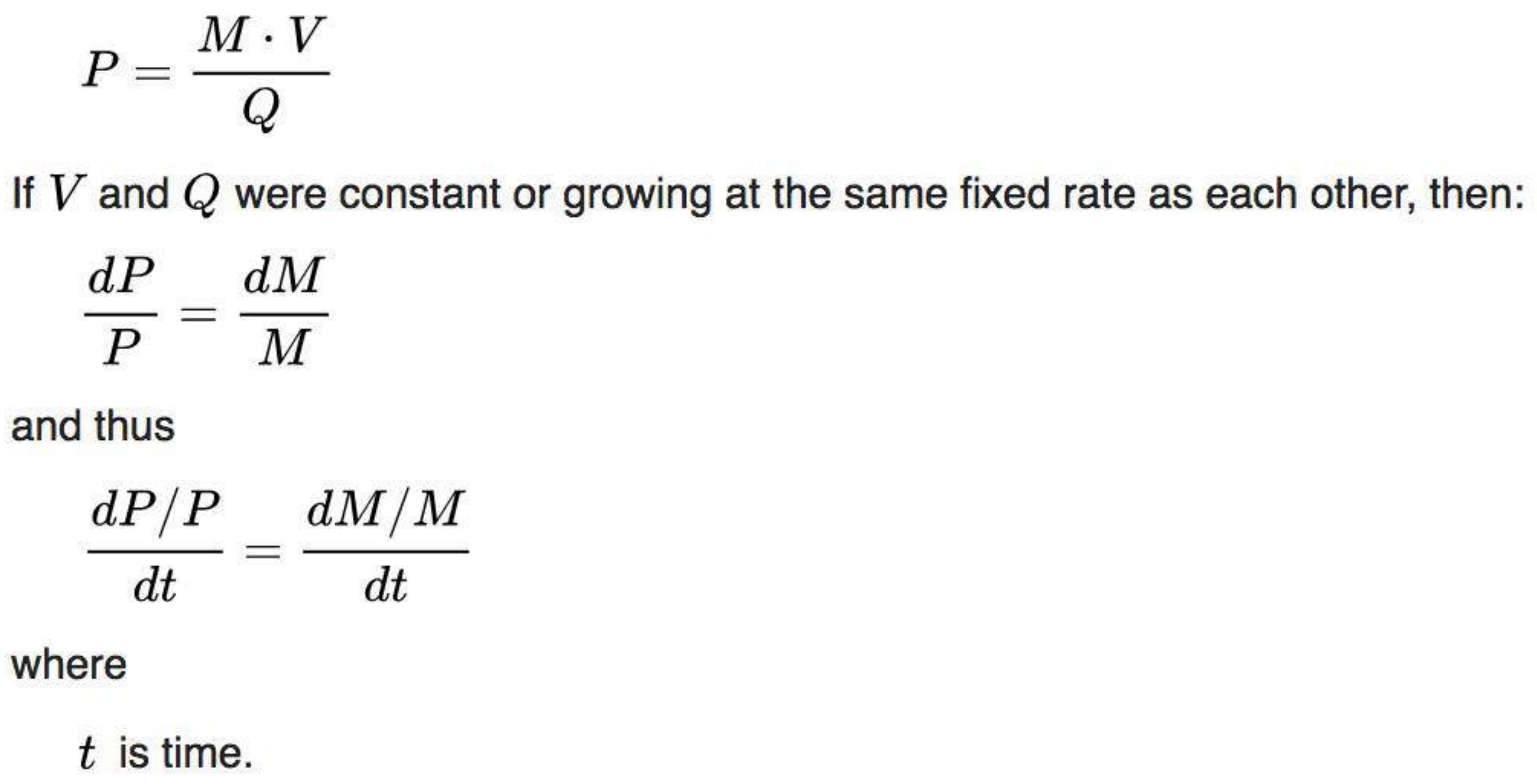
where

p_i and q_i are the respective price and quantity of the *i*-th transaction.

$\mathbf{p}^{\mathbf{T}}$ is a row vector of the p_i .

$\mathbf{q}$ is a column vector of the q_i .

代币的内在价值



$$P = \frac{M \cdot V}{Q}$$

If V and Q were constant or growing at the same fixed rate as each other, then:

$$\frac{dP}{P} = \frac{dM}{M}$$

and thus

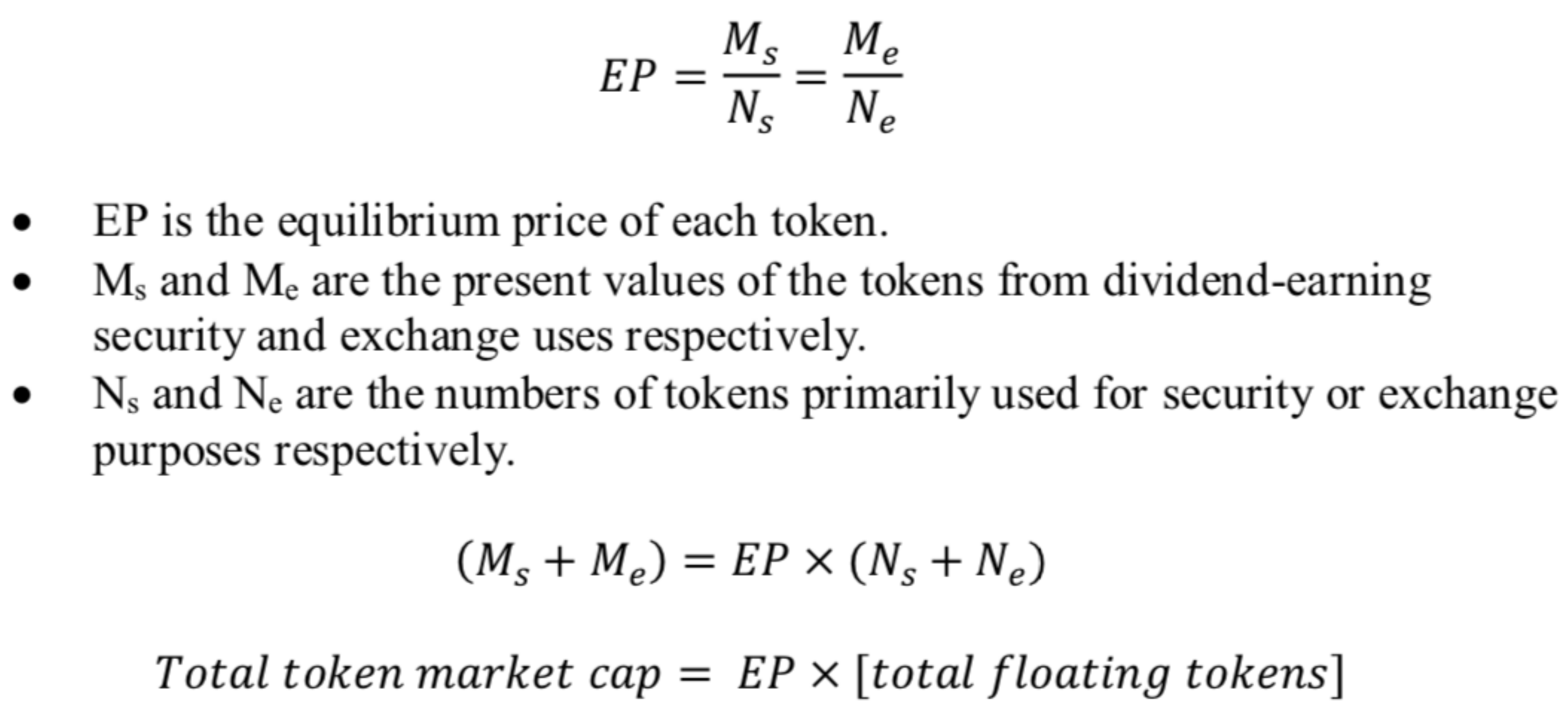
$$\frac{dP/P}{dt} = \frac{dM/M}{dt}$$

where

t is time.

代币的内在价值

A token might have multiple utilities and functions. Their values could be additive.



$$EP = \frac{M_s}{N_s} = \frac{M_e}{N_e}$$

- EP is the equilibrium price of each token.
- M_s and M_e are the present values of the tokens from dividend-earning security and exchange uses respectively.
- N_s and N_e are the numbers of tokens primarily used for security or exchange purposes respectively.

$$(M_s + M_e) = EP \times (N_s + N_e)$$

$$Total\ token\ market\ cap = EP \times [total\ floating\ tokens]$$

证券代币

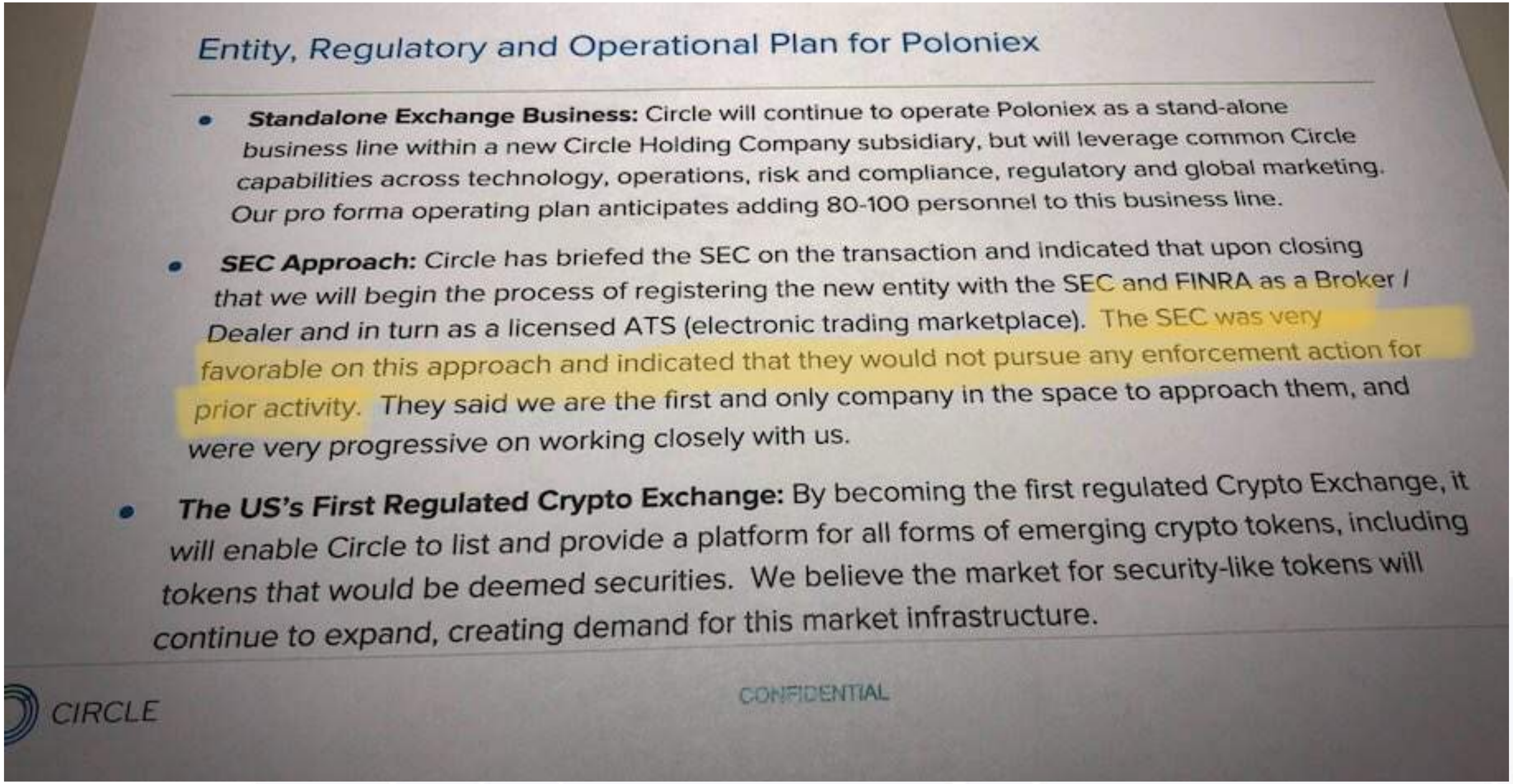
证券代币的场景

- 可编程的股票
  - Eric Ries 的 LTSE
- 使用权的证券化

所有权与使用权

- 所有权的本质是信息的不对称
- 所有权的价值已经在被互联网巨头淡化
- 智能合约有可能覆盖资产的所有使用价值
- 代币是使用权证券化的最好载体

未来已来？



Entity, Regulatory and Operational Plan for Poloniex

- **Standalone Exchange Business:** Circle will continue to operate Poloniex as a stand-alone business line within a new Circle Holding Company subsidiary, but will leverage common Circle capabilities across technology, operations, risk and compliance, regulatory and global marketing. Our pro forma operating plan anticipates adding 80-100 personnel to this business line.
- ***SEC Approach:*** *Circle has briefed the SEC on the transaction and indicated that upon closing that we will begin the process of registering the new entity with the SEC and FINRA as a Broker / Dealer and in turn as a licensed ATS (electronic trading marketplace). The SEC was very favorable on this approach and indicated that they would not pursue any enforcement action for prior activity. They said we are the first and only company in the space to approach them, and were very progressive on working closely with us.*
- ***The US's First Regulated Crypto Exchange:*** *By becoming the first regulated Crypto Exchange, it will enable Circle to list and provide a platform for all forms of emerging crypto tokens, including tokens that would be deemed securities. We believe the market for security-like tokens will continue to expand, creating demand for this market infrastructure.*

CIRCLE

CONFIDENTIAL

主办方 Geekbang 极客邦科技 InfoQ

GMTC2018

全球大前端技术大会

大前端的下一站

<<扫码了解更多详情>>

扫码关注

获取更多培训信息

Growing **Technicians**

Growing **Companies**