

数字社会 (Digital Society): Computational Legal Studies

蔡维德 Wei-Tek Tsai
北京航空航天大学 &
亚利桑那州大学

概述

- 介绍与动机
- 计算法律研究
- 智能合约
- 数字ID与自主管理
 - ID3, 架构, OpenPDS, OMS (开放芥子)

简介

- 我们正在步入数字社会，在这里，除了电子邮件、网站和博客外，还做其他数字化的事情。
- 在数字社会中，我们可以做到合法交易，如银行交易、买卖商品如房产和股票、备案诉讼、结婚、离婚、出生、死亡、学位证书，设置遗嘱、发行成绩单，和护照申请等。
- 这是一个新的研究领域，它涉及到许多学科，例如计算机、法律和商业。
- Earlier, L. Lessig proposed Code 2.0, code is the law.

作为新学科的“数字社会”

- 它是一个**计算架构** (computational architecture): 这种架构是可以运行的。架构涉及到信任 (trust)、声誉 (reputation)、区块链 (blockchains)、数据库 (databases)、机械学习 (machine learning), 货币 (currency), 和**可执行**的法律 (executable law) (如智能合同 smart contracts)。
- 它涉及到现实生活中的实体, 如政府、银行、股票和国债、公安、法院、医院、学校 (从幼儿园至研究生院) 以及和公司。
- 与虚拟的电子游戏不同的是, 在这个数字社会中, 每一件事都是**真实**的、**合法**的。

以金融科技学作样本

- 由于2009年出现的比特币以来，FinTech（**金融科技学**）成为一个热门的投资重点，如今英国伦敦认为金融科技学仅在工作这方面就能够达到全市预计十万份工作岗位要求。
- 国外各大银行（包括美国中央银行和商业银行等），重大证券交易所（**NASDAQ, NYSE**），期货交易所等都在参与投资金融交易学。
- 英国政府和**IBM**本月刚刚宣布以金融科技学为主的重大的合资企业，**IBM**已经同意用她最强大的推理引擎**Watson**作为该合作计划的一部分。

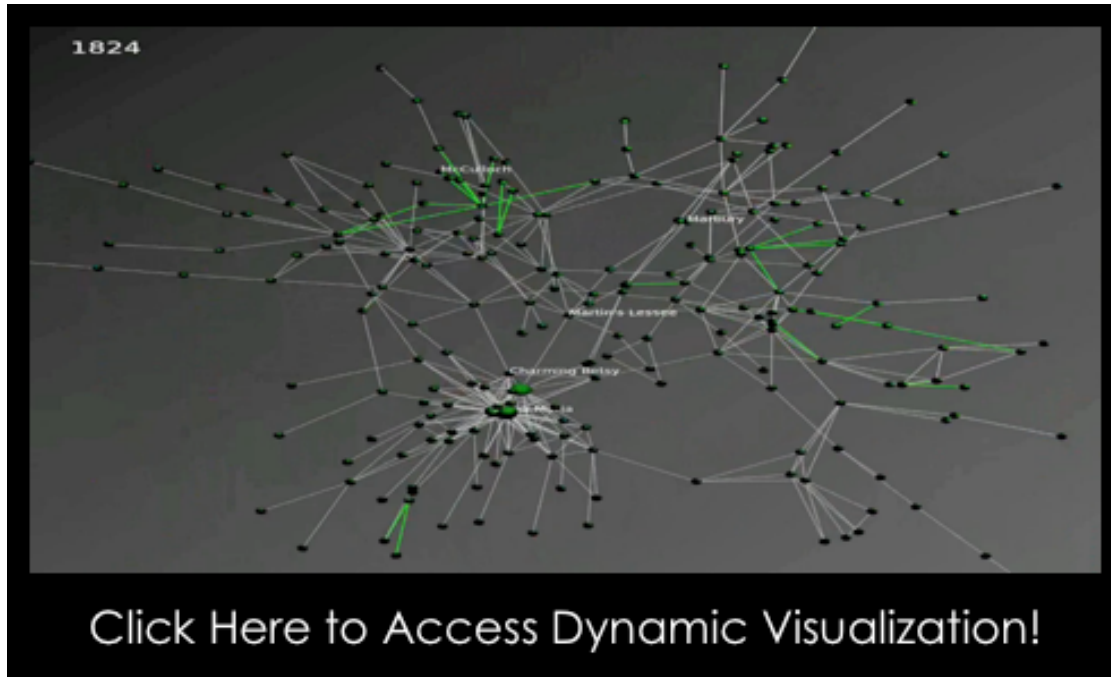
概述

- 介绍与动机
- 计算法律研究
- 智能合约
- 数字ID与自主管理
 - ID3, 架构, OpenPDS, OMS (开放芥子)

计算法学

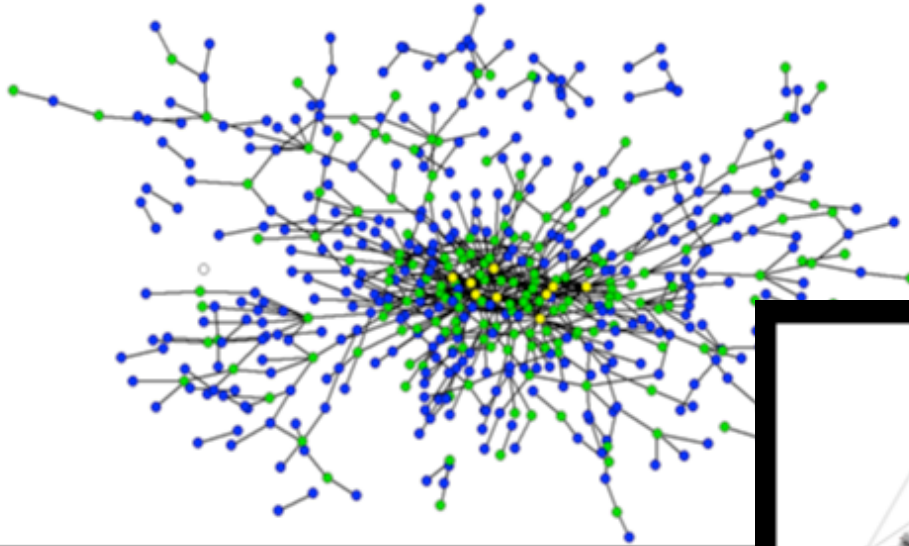
- 计算法学是一种适用于计算法的新学科。这始于**1987**年由斯坦福教授领导了这个领域。他的分析方法分为三部分：
 - 实证分析 (empirical analysis)
 - 计算法律 (Algorithmic law)
 - 形象化，可视化 (visualization)
- 数字社会 (digital society) : from Internet+ to within-Internet

英国普通法的网络分析

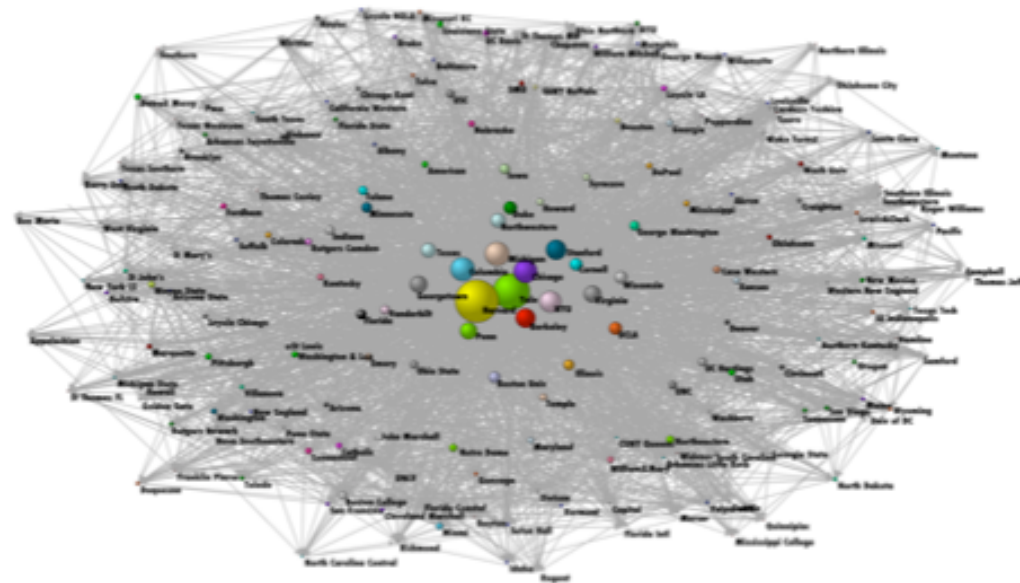


英国普通法的演变，每一个链接表示他们在法律过程中的关系。这表示了司法行为附加到先前决定的优先权。

美国法律的网络分析



[Click Here to Access Zoomable Visuali](#)

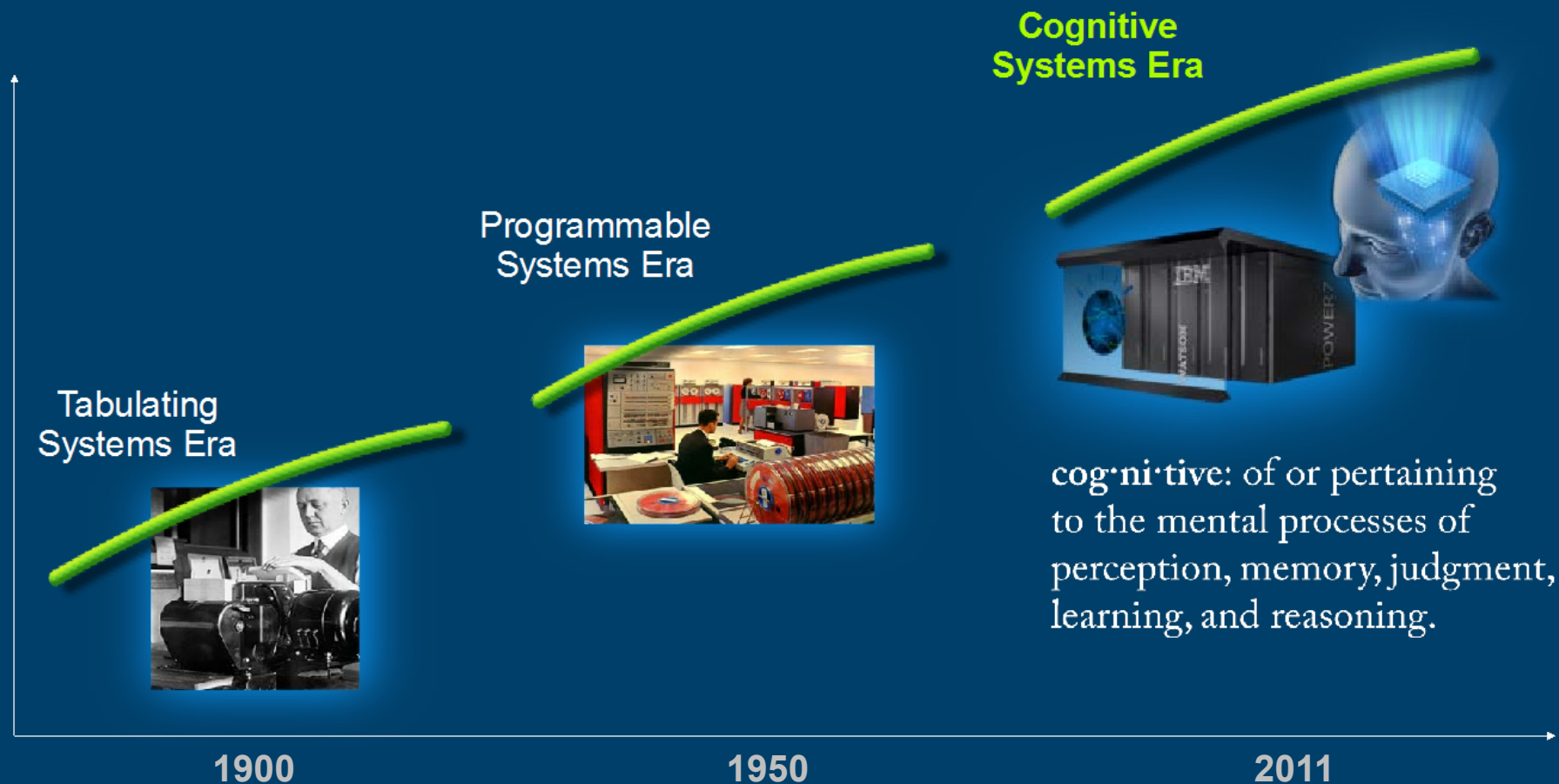


[Click Here to Access Zoomable Visualization!](#)

计算法学研究

- 2015年6月22日，IBM宣布她将运用Watson软件来分析法律契约合同。
- 2011年，IBM的Watson软件成为世界第一个能解决有“常识”问题的软件，在这之前一直这被认为这是不可能的。这是IT领域一年中最重要的消息。
- 现在，它被应用到许多不同的领域，如医疗保健（癌症）、法律、商业和许多其他领域。
- <http://computationallegalstudies.com/2015/06/ibm-watson-for-contract-analytics-at-legal-onramp-via-ron-friedmann/>

Watson正迎来一个新的计算时代. . .

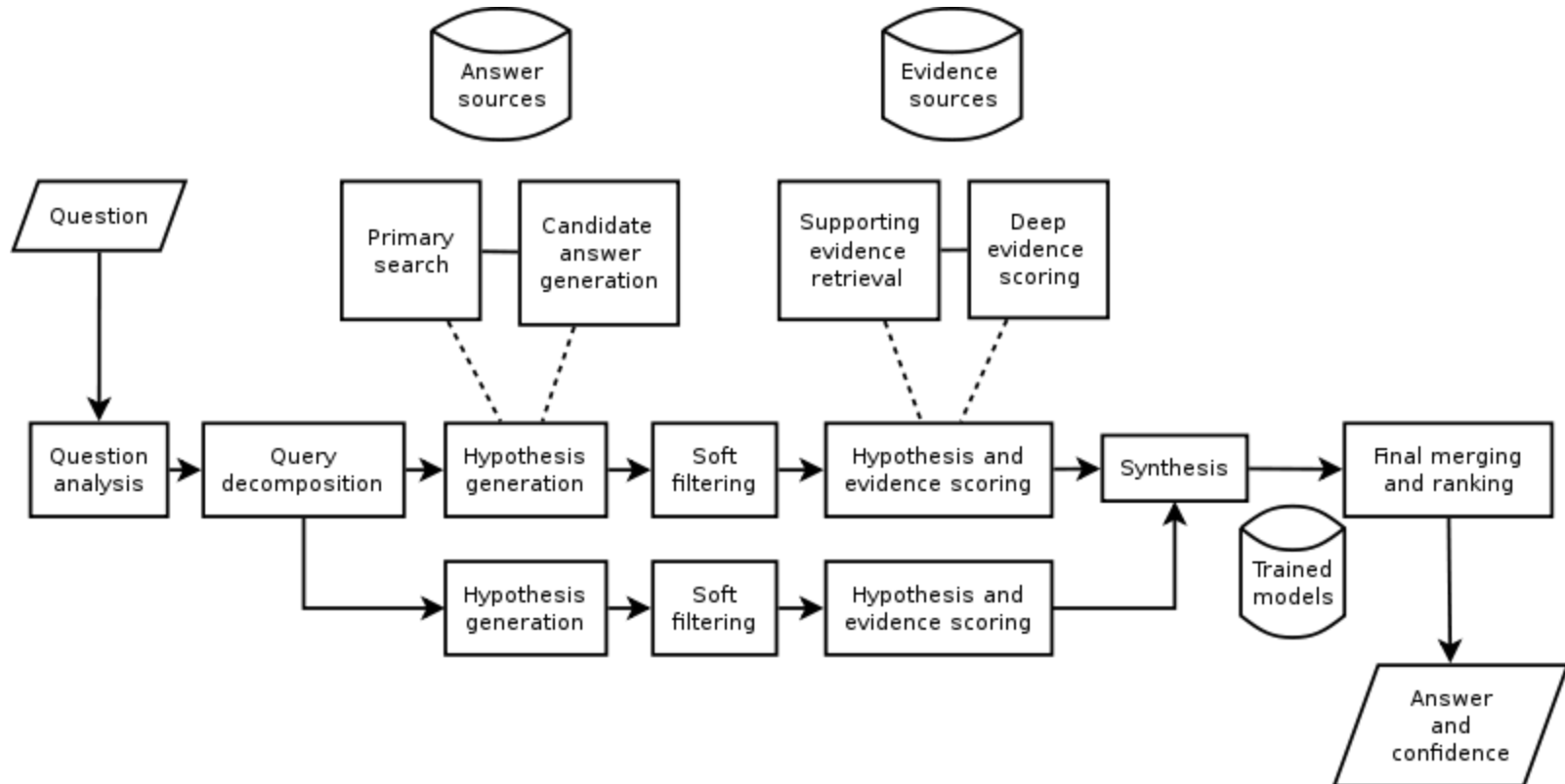


。 。 。 启用新的可能性和结果

Data Stored as Ontology

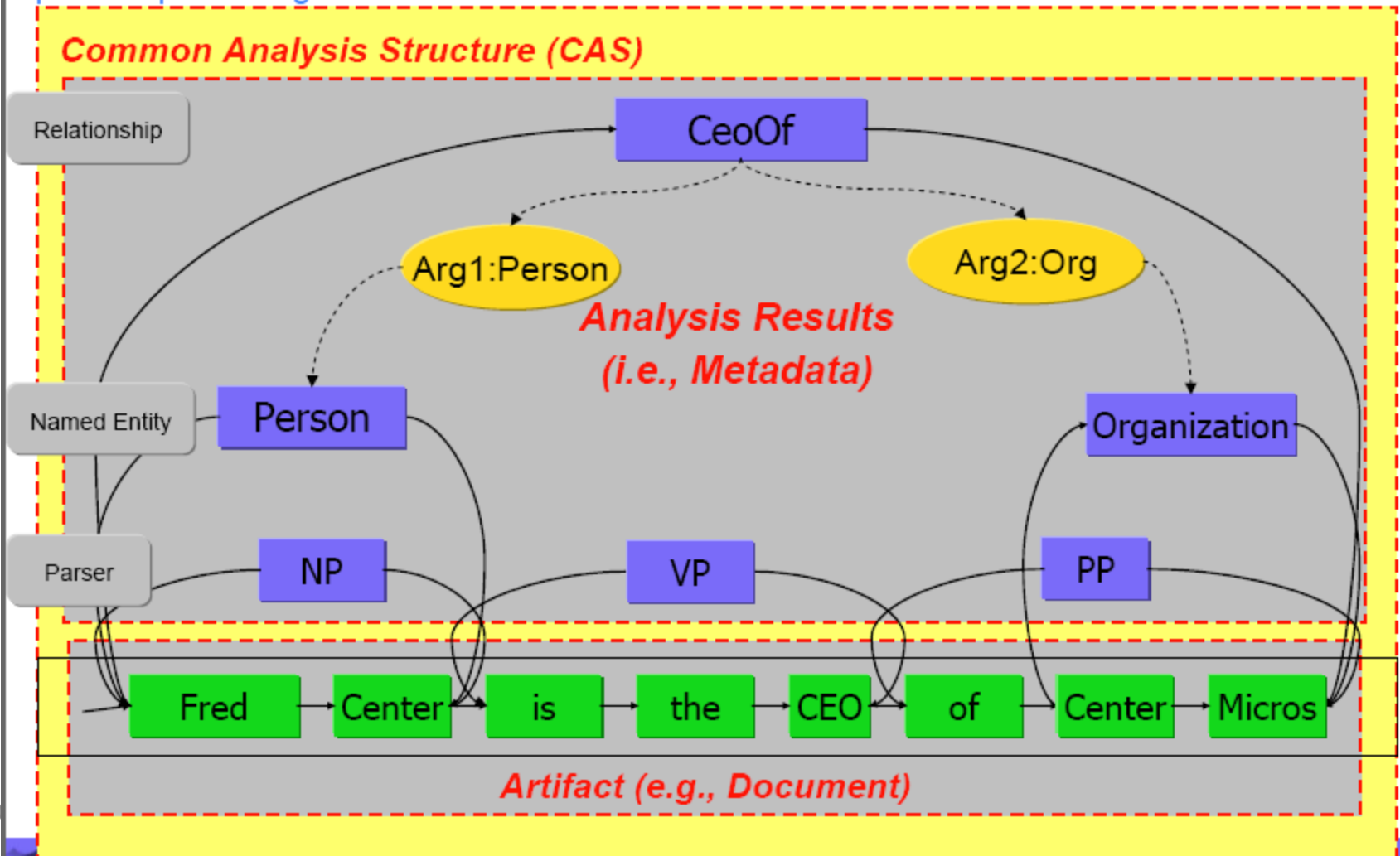
- The sources of information for Watson include encyclopedias, dictionaries, thesauri, newswire articles, and literary works. Watson also used databases, taxonomies, and ontologies. Specifically, [DBPedia](#), [WordNet](#), and [Yago](#) were used.
- DBPedia is an ontology based on Wikipedia, WordNet is a dictionary, Yago is a database contains knowledge harvested from Wikipeida with 95% accuracy.
- Watson contained 200 million pages of structured and unstructured content consuming four terabytes of disk storage, including the full text of [Wikipedia](#).

IBM Watson Internal Processes



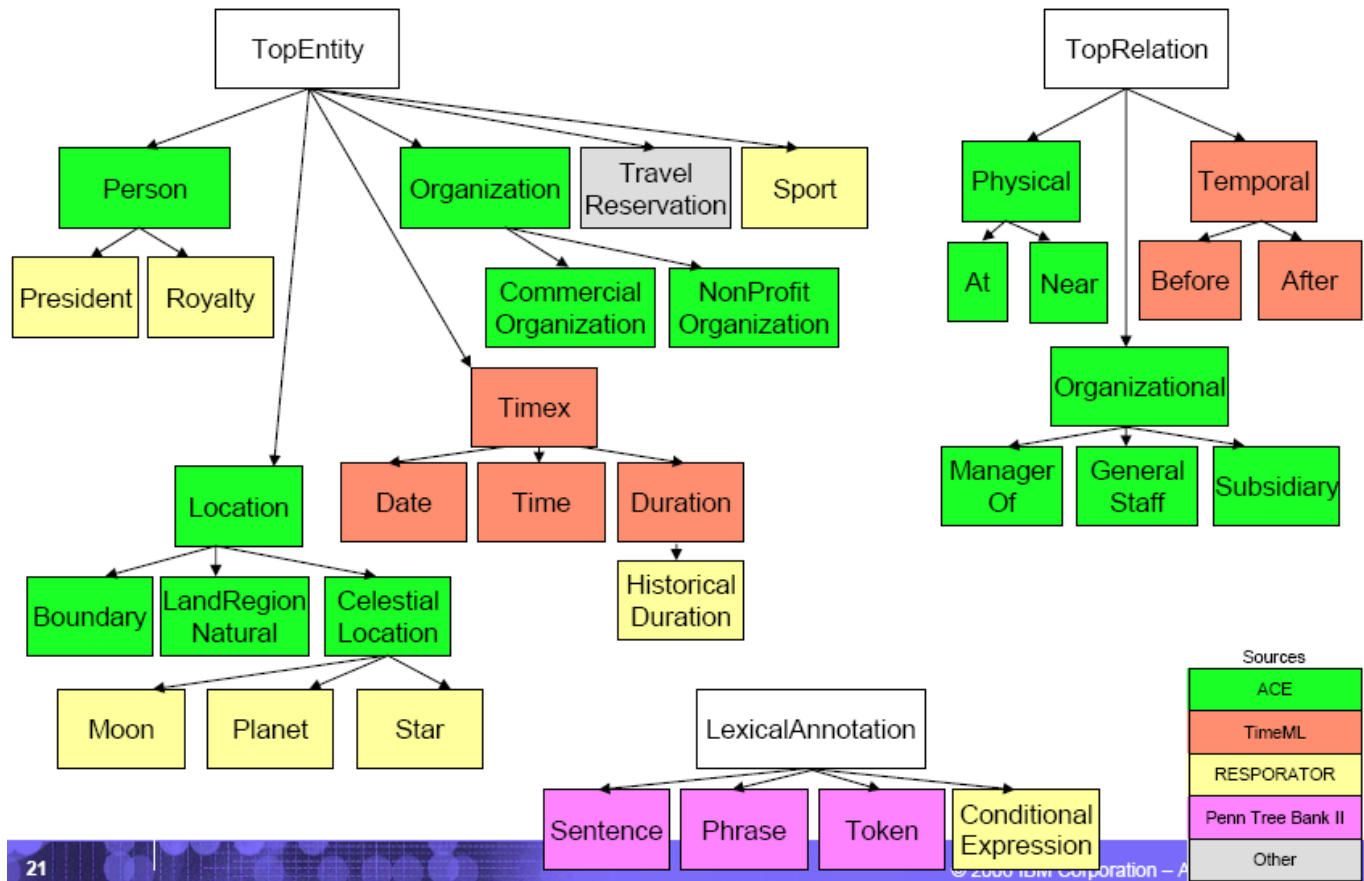
UIMA Natural Language Processing

UIMA's Basic Building Blocks are **Annotators**. They iterate over an artifact to discover new types based on existing ones and update the **Common Analysis Structure (CAS)** for upstream processing.



Generated Ontology from UIMA

Partial *HUTT* Type System (254 concepts in total)



UIMA Annotation Tool

The screenshot displays the UIMA Annotation Viewer interface. The main window shows a text document with various annotations highlighted in different colors. A legend at the bottom left lists the annotation types: Person, Facility, GPE, Organization, GeneralStaff, BasedIn, and Management. The right pane shows the details of the selected annotation, which is an Organization ("Gorman Food Importers Inc.") with a componentId of ACE. A yellow callout box labeled "A CAS" points to the text and the annotation details, with a red dashed arrow pointing to the "componentId = IBMEAnnotator" field.

UIMA Annotation Viewer

Report Date 10 March 2003. Slick business dealings keep local olive oil importer out of the pits. Robert Crane was recognized by local business leaders for his skill at leading the Gorman Food Importers Inc. to strong profits while others are struggling. Mr. Crane, owner of Gorman Food Importers Inc., has consistently been able to produce exceptional results, while still keeping a focus on his employees. Gorman Food Importers Inc. has been in business since 1970 and specializes in food imports from the Middle East, including olive oil and figs. Gorman Food Importers Inc. is headquartered in NYC, and their warehouse is located in Paramus, NJ. The company employs 659 people in the two locations. Robert Crane can be reached at 608-703-2317.

Click In Text to See Annotation Detail

- Organization ("Gorman Food Importers Inc.")
 - begin = 185
 - end = 211
 - componentId = ACE
 - mentionType = NAME
- Organization ("Gorman Food Importers Inc.")
 - begin = 185
 - end = 211
 - componentId = IBMEAnnotator
 - mentionType = NAME

Legend

<input checked="" type="checkbox"/> Person	<input checked="" type="checkbox"/> Facility	<input checked="" type="checkbox"/> GPE	<input checked="" type="checkbox"/> Organization	<input checked="" type="checkbox"/> GeneralStaff
<input checked="" type="checkbox"/> BasedIn	<input checked="" type="checkbox"/> Management			

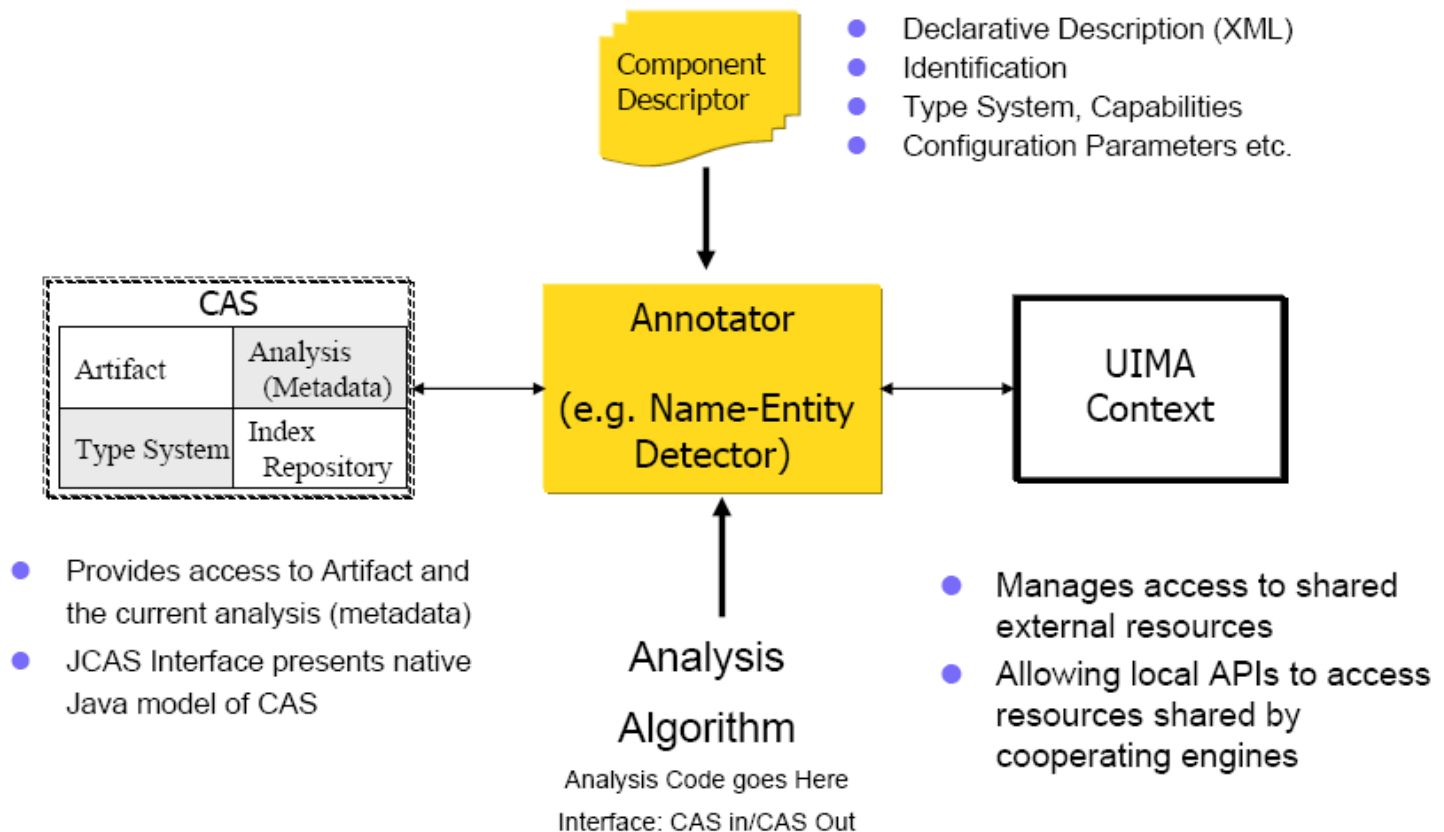
Select All Deselect All Viewer Mode: ☒ Annotations

A CAS

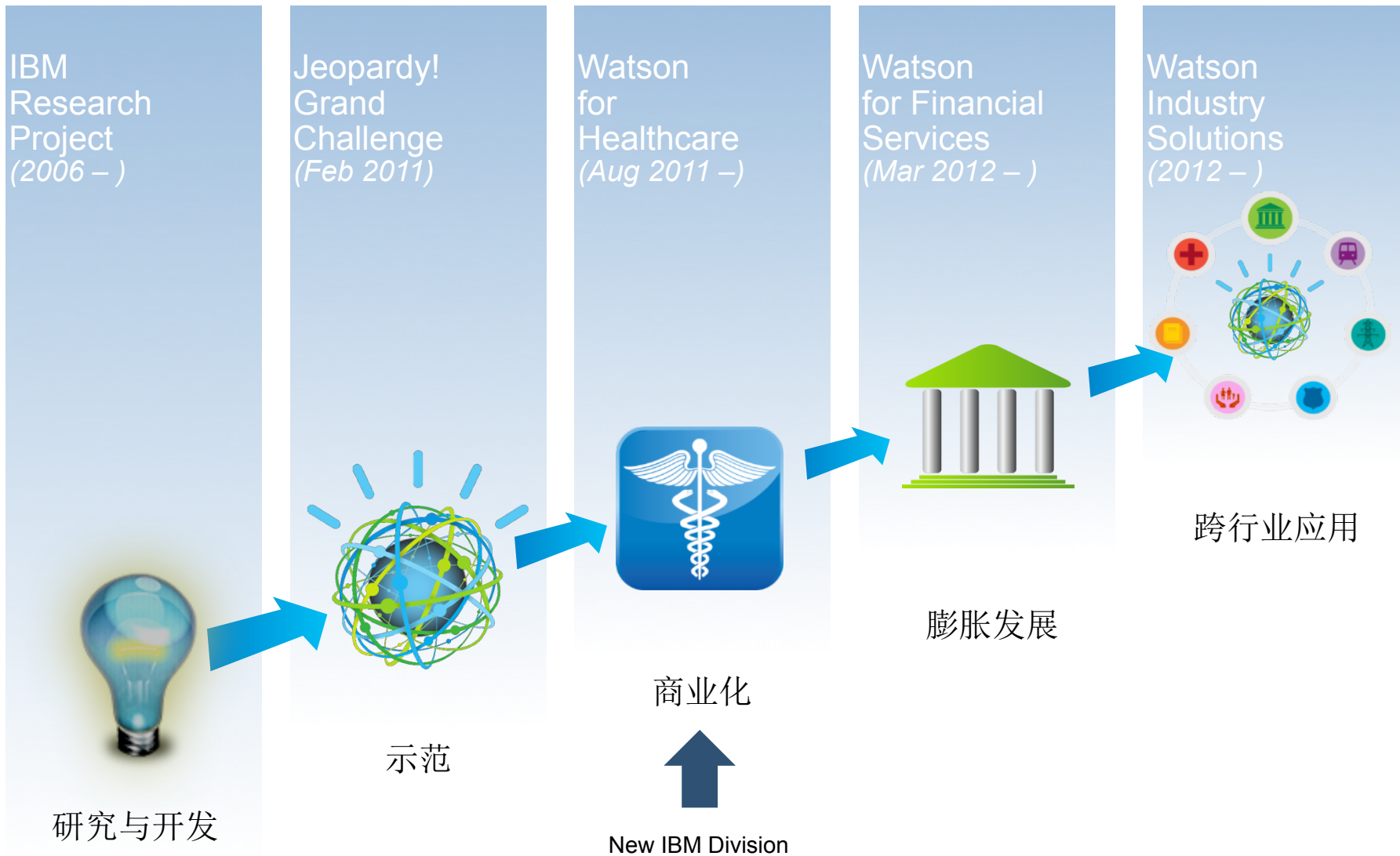
- Analyzed by a combination of Analysis Engines
- Semantic Entities & Relations Represented
- Highlighted here in a GUI

UIMA Capabilities

The Basic UIMA Component Interfaces



IBM Watson的简要发展历史

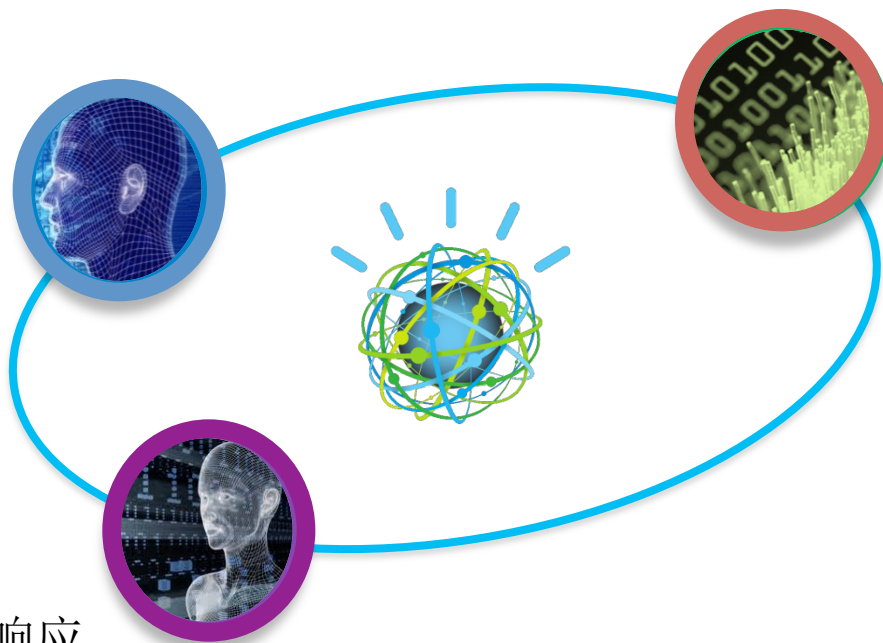


IBM Watson 联合转换技术

1 理解自然语言
和人类交流

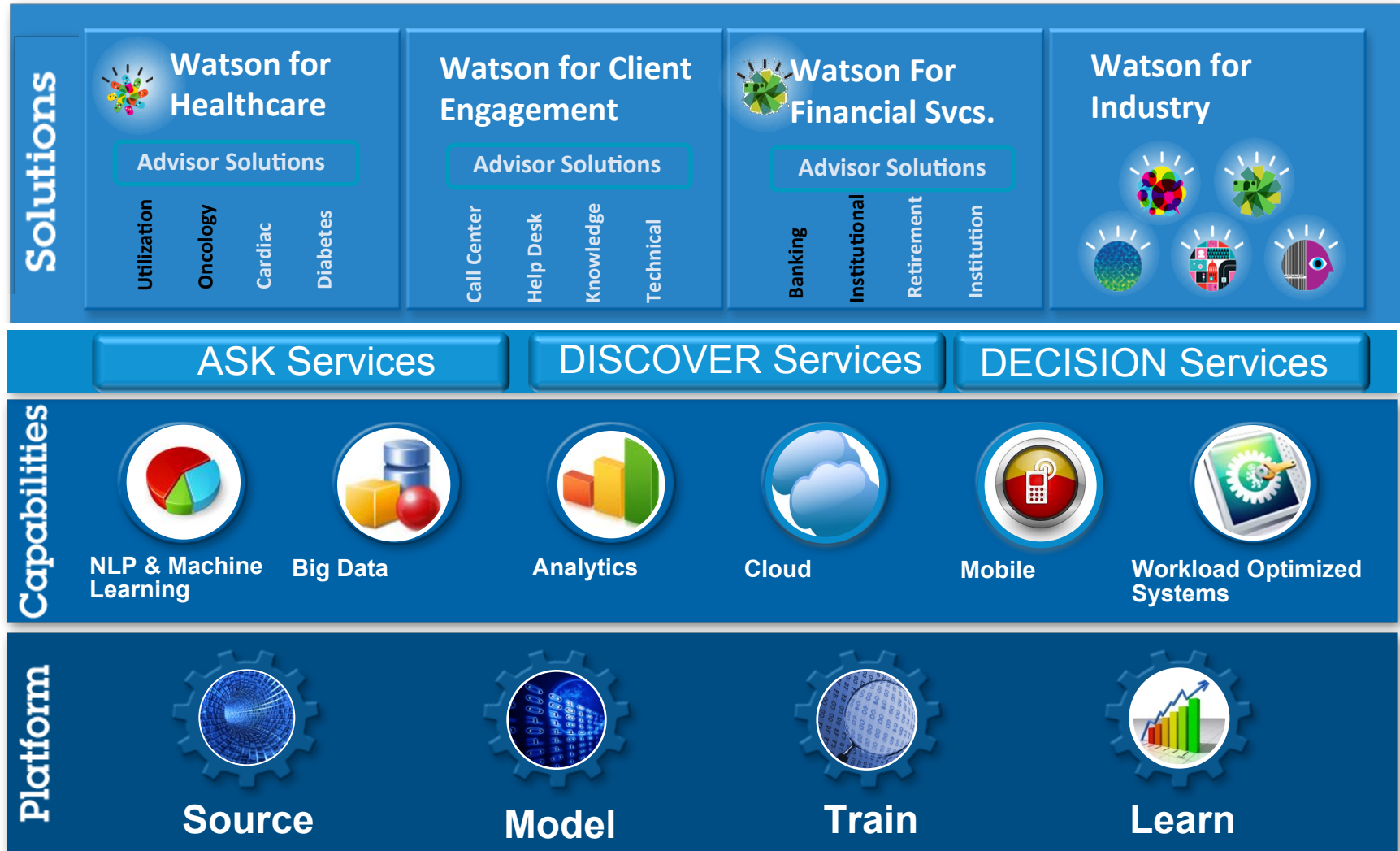
2 生成和评估
循证假说

3 适应和学习
用户的选择和响应



*...built on a massively parallel
architecture optimized for IBM POWER7*

产品和基础设施



“Watson律师”将出现

- 2014年8月，在International Legal Technology Association年会和IBM讨论在未来Watson将如何出现在法律中。
- “Watson律师” (legal Watson) 将取代初级员工或者至少完成他们的大部分工作。他的成功取决于以下三个问题的答案：
 - Q1: 什么样的信息—多少信息—Watson律师是否必须提取？必要情况下，将由谁来调整？
 - Q2: 如果Watson律师得到足够的调整，它能否行驶正确的法律判决？能不能够为客户产生正确的法律意见？
 - Q3: 它所产生的法律是否是正确合理的？并且谁会行使它所产生的法律判决？
- 2015年6月22日，“Watson律师” 软件来分析法律契约合同

概述

- 介绍与动机
- 计算法律研究
- 智能合约
- 数字ID与自主管理
 - ID3, 架构, OpenPDS, OMS (开放芥子)

智能合约 (Smart Contract)

- 智能合约: 计算机执行或验证合约。
- 智能合约最初由Nicholas Szabo研发 (有些人认为他就是比特币的Satoshi Nakamoto), 他有法律和计算机的背景。
- Before we look at smart contracts, we need to take a look what was done before.

Selectica 合约管理流程



软件过程是通过 CPQ（配置价格报价 **configure, price, quote**）进行的，这是一个创新的软件需求过程。该公司首先开发了一个全面的具有重要的法律知识的合集，并且每一个合同都是一**致性**和**完整性**的子集，并且合乎当今法律的。

讨论

- Selectica是一个伟大的过程和思想，但首先需要开发出大量的知识和存放在数据库里面来完成合同。并且随着法律的变化，来完成合同的软件也需要迅速改变。
- 它以前是没有用到区块链，并且它的产品得产生是基于传统的文本，因此它的合约是不能被计算机执行的。
- 在网络上, Selectica和法律形式 (legal form)和模板 (template)竞争，它们把大量的法律模板文件放在网上由大家进行改动。
- They key is that they are not executable. Preparation, analysis, and production can be computer executable.

相似技术

- **数据库触发器 (database trigger)**: 一个软件被连接到一个数据库中, 当一个数据被改变, 满足一个触发条件时, 该软件附带的触发器将被自动执行, 包括在数据库中的数据的变化。
- **在安全系统或服务系统执行的策略 (policy in secure systems or service systems)**: 政策表示声明或使用执行语言来表示, 当特定事件发生的情况下, 符合该策略, 那么策略将执行。例如, 当某人需要调用某服务时, 托管系统可能会运行一个策略检查以确保该调用是否方有权调用服务。可以查看WS-*论文, 我的论文。
- 关键在于, 执行方面并不是一个问题, 并且在计算机方面已经做了许多年。但在法律方面, 它却是很重要的。

数字社会中的智能合约

- 很多加密货币系统2.0具有智能合约并且与区块链有关系，而区块链可能包含具有潜在价值的数字资产（例如股票，人民币或黄金），或连接到的物理量（如性能）。其中大部分有编程合同和执行基础设施，以实现智能合同。
- 问题是，什么样的合约可以被称为“智能合约”？智能合约并不是因为他的“执行”展现出智能。

“智能”合约 5 项原则

- 原则1: 存储在智能合约中的所有资产项目必须合法且有效的，运行的单位或个人在法律上必须要拥有合法的所有权。
 - 例如，由 “Waston律师” 验证，所有的资产都是合法的。
- 原则 2: 智能合约的程序必须是被法律认同的程序，以使它具有法律效力，
 - 例如, 程序是否被律师, 法官或 Watson 律师所承认?

“智能”合约 5 项原则

- 原则 3: 执行正确.
 - 由智能合约计算所产生出来的结果是不是正确？且是不是具有法律根据的呢？
 - 或者程序是正确的，可是在执行时被动了手脚，有资产被挪用，或是在执行时发生故障，
 - 有步骤发生错误，该如何更正？
- 原则 4: 智能合约的结果存储具有法律约束力。
- 原则 5: 智能合约的结果 can be stored reliably and without any change.
- Smart Oracle

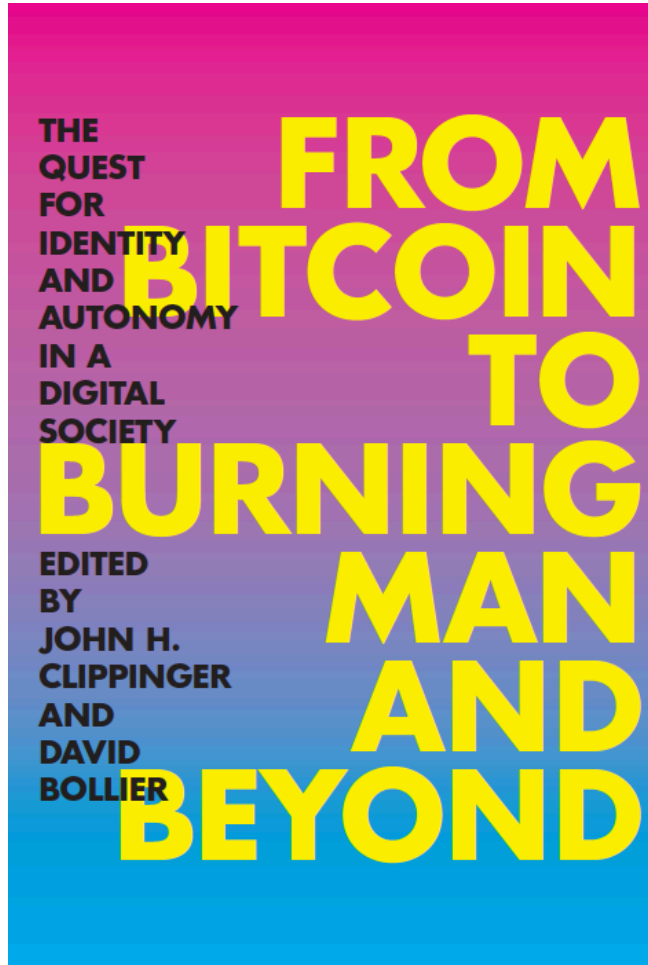
“公开交易” (open Transaction) 中的 “智能合约”

- 一个智能合约可以被激活，一旦激活，它就能自主运行。
- 它有可执行代码，涉及多个当事人。
- 只有被选定的功能可被用作可执行代码。
- 它可以只操纵那些被明确声明的合法资产。
- 它可以暂时储存资金。
- 合同的状态被记录。
- 智能合同中的所有变量 (variables) 是持续的 (persistent) 不断的 (unchangeable)。

概述

- 介绍与动机
- 计算法律研究
- 智能合约
- 数字ID与自主管理
 - ID3, 架构, OpenPDS, OMS (开放芥子)

麻省理工学院的数字社会



这是麻省理工学院媒体实验室在2014年时所做的工作，主要是数字ID和自主性。

ID3= Data-Driven Design

可免费下载于
idcubed.org/bitcoin-burning-man-beyond/

Windhover的数字身份, 信任和数据管理原则

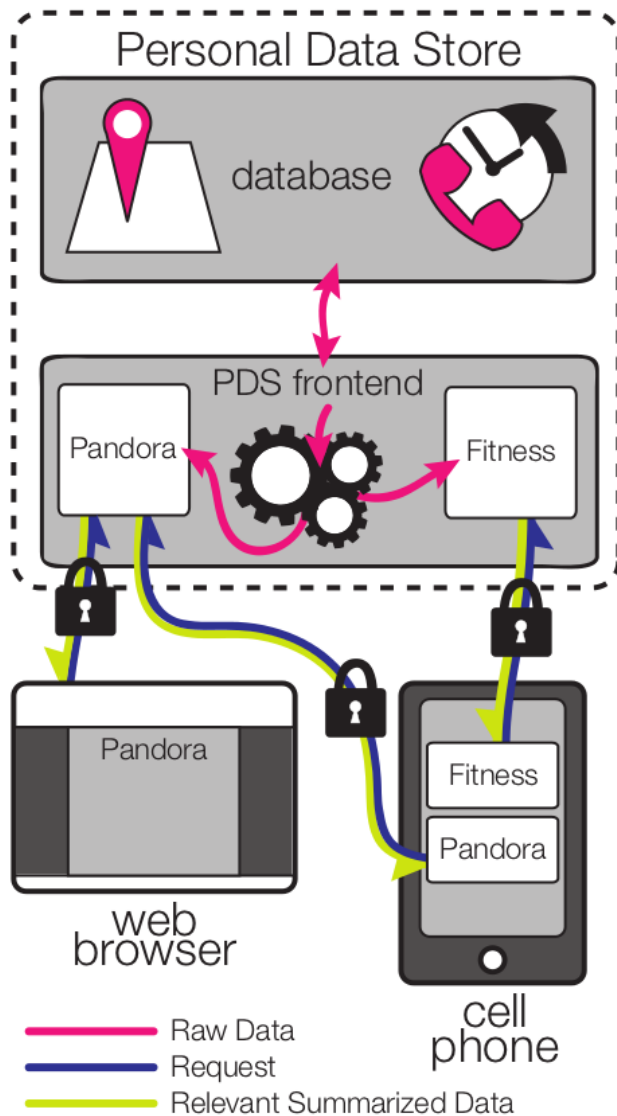
- Windhover Principle of Digital Identity, Trust and Data)
- 1. 数字身份与个人数据的自我控制主权(Self-Sovereignty of Digital Identity and Personal Data):
 - 个人应该控制自己的数字身份凭证和个人资料，而不是由社会网络、政府或企业来掌控。实现数字社会，加强创新数字技术，应该以提高隐私的管理和实施为首要任务。
- 2. 适当实施基于风险的监管（Proportionate Enforcement and Risk-Based Regulation）：
 - 加强个人隐私的管理，改善可调节性的法律审计以及加强法律的执行力度。

Windhover原则

- 3. 在信任机制和隐私保护方面要确保创新(Ensuring Innovation in Trust and Privacy) :
 - 一个有效的自主识别系统，需要反复加深信任、安全、治理、问责和隐私。
- 4. 开源创作与持续创新(Open Source Collaboration and Continuous Innovation):
 - 用一个包容的、开源的方法构建系统来体现这些规则。

ID3 框架

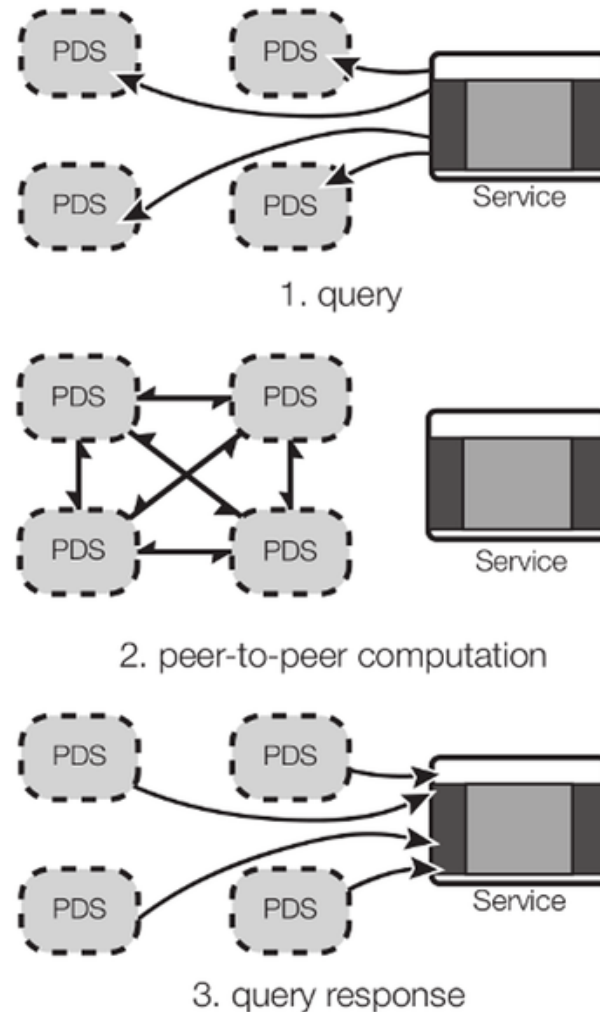
应用 (Applications)
核心服务 (Core Services)
信任框架 (Trust Framework)
身份管理与认证 (ID Management and Authentication)
核心身份证 (Core ID)



Openpds（个人数据存储）是一个开源的应用软件，是一种基于ID3算法的原理，从openpds.media.mit.edu开放源码应用程序。

其中最重要的原则是，它输送的只是软件和计算结果，并不是把原始数据输送出去，从而保护了个人隐私。因为通过通过原始数据，如位置信息，将很容易识别别人。

Figure 5. Group Computation Overview.



为了要保护个人的隐私，可以把人们不同的信息分别存储在各个不同的PDS中，而各个PDS可以互相沟通来获得信息，从而回应顾客的需求。

D. P. Reed's Law

- 广播模式 (broadcast), 可以实现消费者的消费需求。
- 对等模式 (peer-to-peer): 相互作用变成 N^2 。
- 团体 (community): 每个人都是自由加入任何团体, 和相互作用成为 2^N 。
- 为了达到这一水平, 我们需要一个新的架构来支持GFN (集团形成网络)。

群体构建形成的网络

Figure 3 - Dominant Value Regions

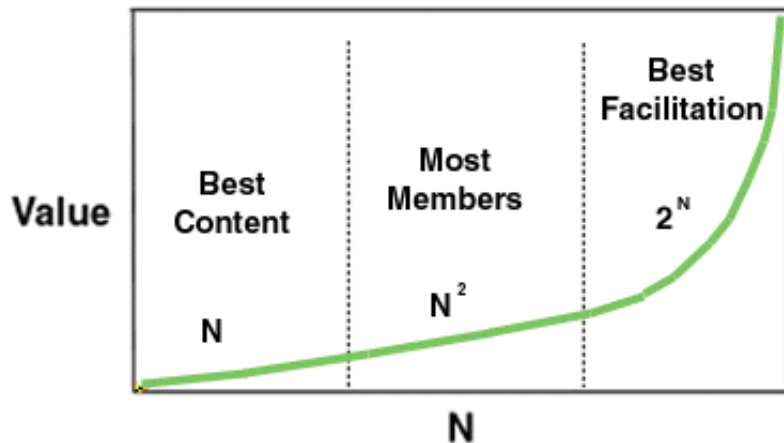
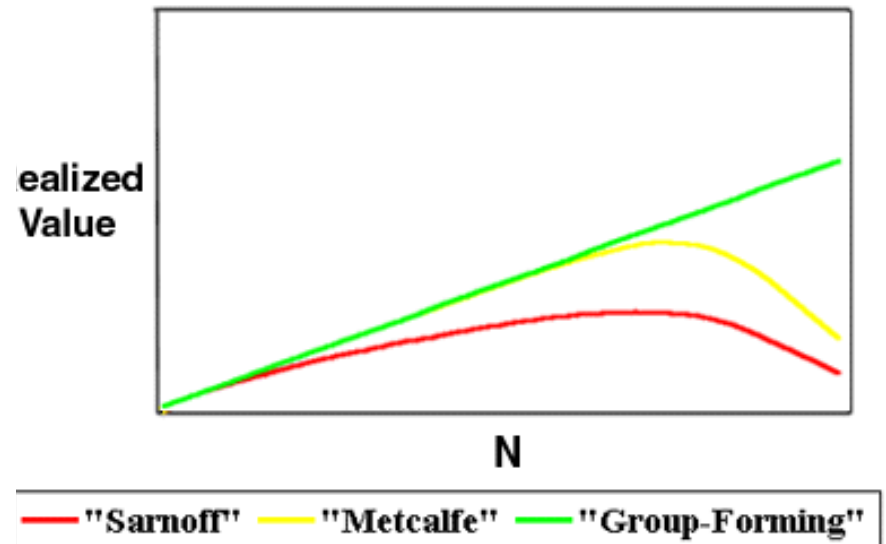


Figure 4 - Saturation



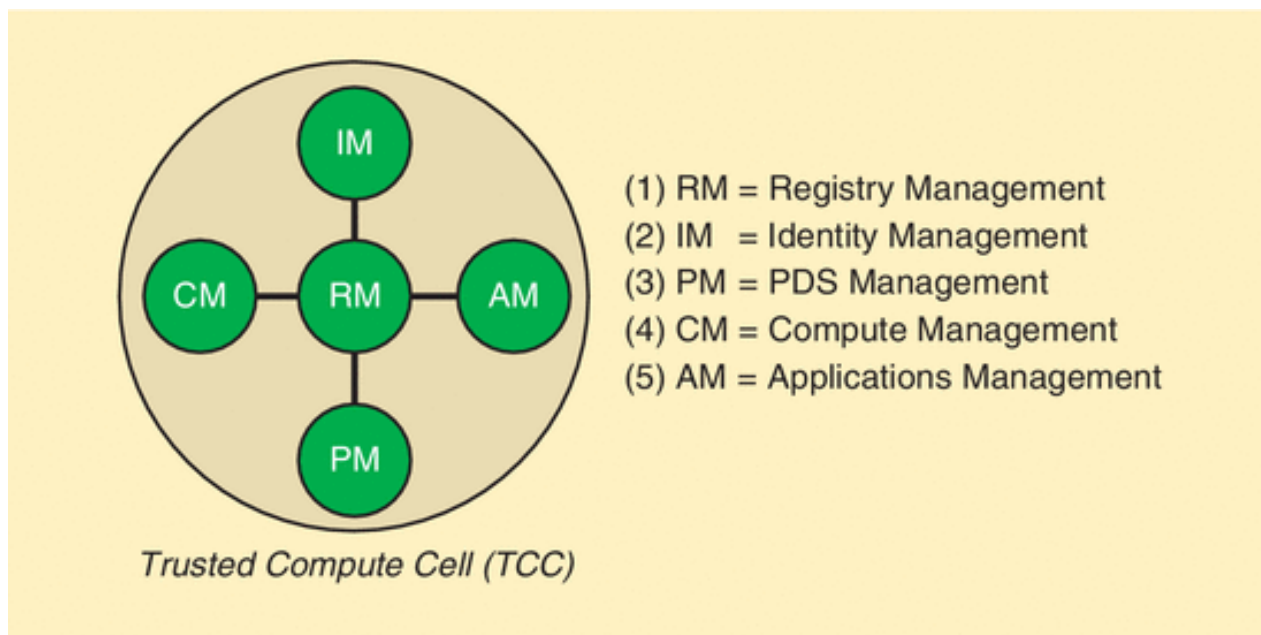
开放式芥子结构

- 一个开源框架，用于开发和部署安全和可信的云计算和移动应用。它提供了一种新的自主部署和自主管理的网络基础设施层，使个人对自己的身份和他们的数据进行控制。
 - 自主组织，分权自治组织，权威机构，创造和自由交换“数字资产”以及个人信息。

OMS (Open Mustard Seed)开放芥子

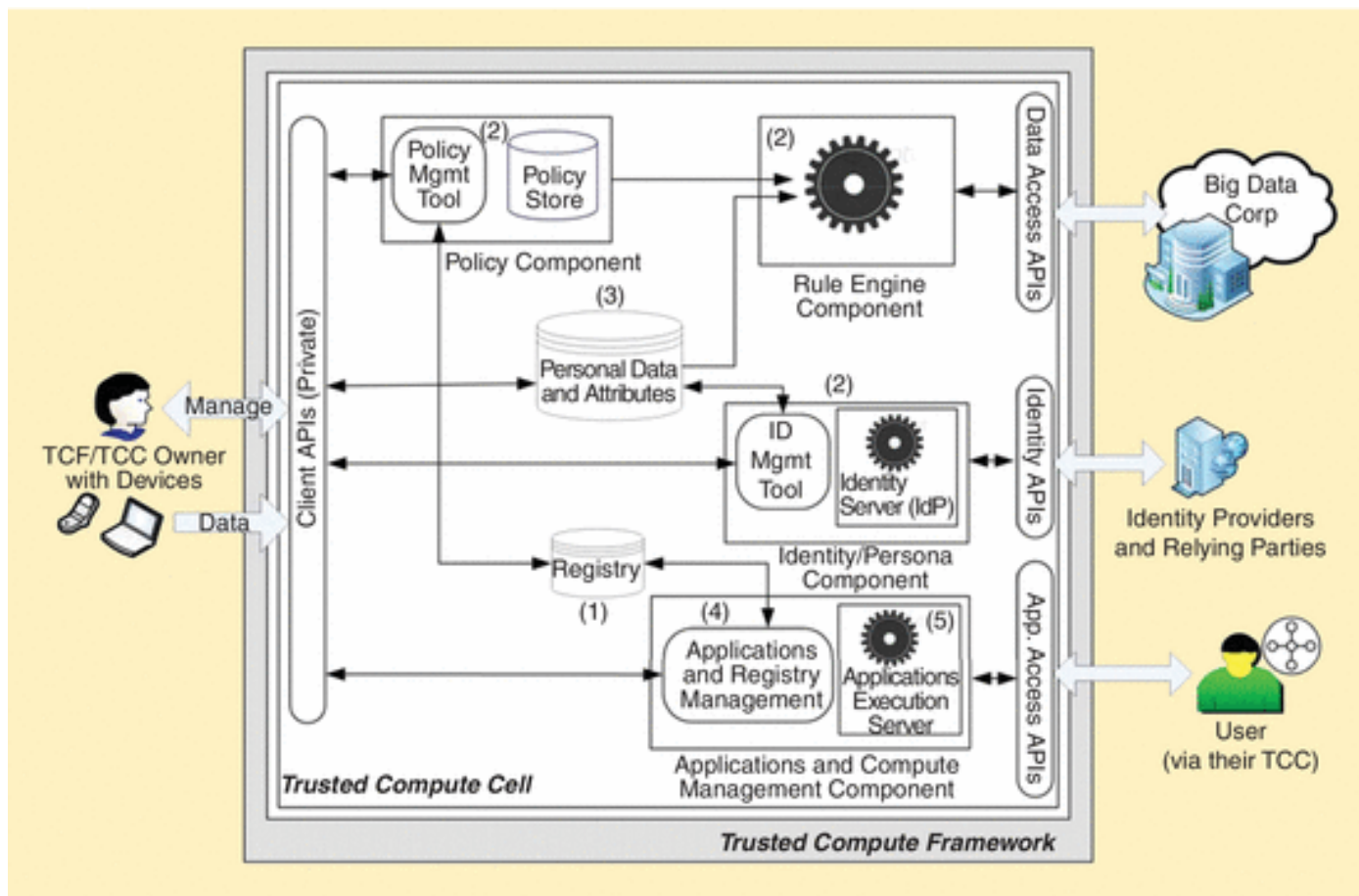
- OMS集成技术包括可信的执行环境、区块链2.0、机械学习，和安全的移动和云计算。
- 提供个人数据服务（PDS）结合OpenID连接云存储，共享，和安全计算。
- 存储、部署、计算、发现、数字货币的服务、托管服务、审计及合规记录，和市场交易自动化。
- 按设计原则实现了公开认证和“隐私设计”原则。
- 允许用户授权执行分散的数字资产和网络服务的智能合同。

可信任的计算单元



TCC (Trusted Computing Cell) 是由5个模块组成的原子单元，由多个单元组成一个框架，它可以构成TCF。它看起来像一个代理或中介，或一个积极主动的服务。

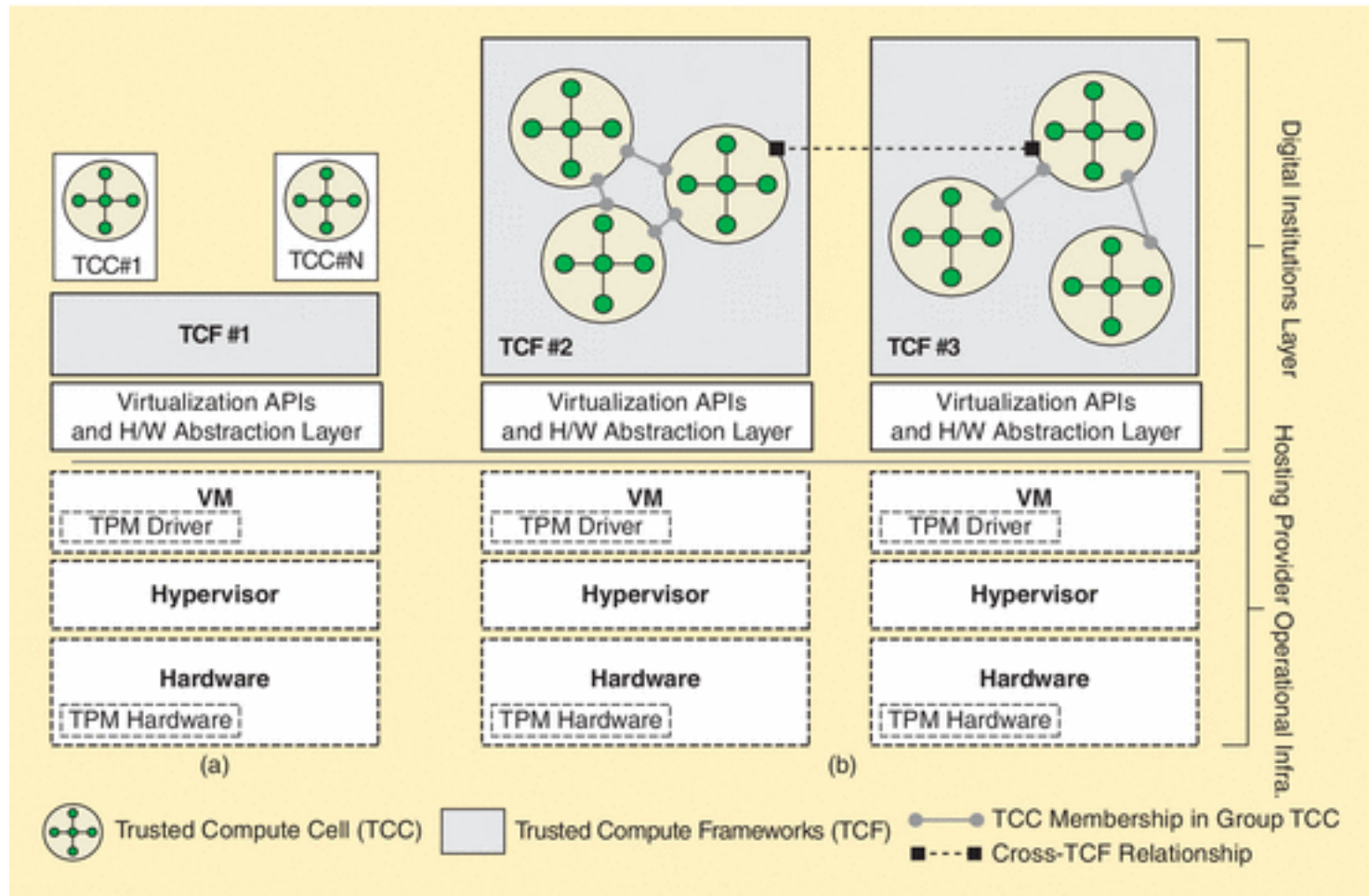
可信任的计算单元(TCC)



可信的计算框架(TCF)

- 它是一个可移动的单位，它可以由所有者的云储存组成，它也可以被转移到另一个云平台。它具有以下功能：：
 - TCF管理
 - 虚拟机配置和管理
 - 框架和引导
 - 政策和应用管理
 - 安全与自我保护

TCC (Cell) and TCF (Framework)



Data Common 和数字法律

- 诺贝尔奖的得主Ostrom提出，一个自主单位能够管理所共有的资源。
- 而数字法律可以经由智能合约执行，来检测内置的腐败和内部勾结的检查。
- 因为每个团体都会有它自己的法律，所以这将是动态的，结果为**导向的**，它可能会发展像**摩尔定律**。

自主组织管理的团体

- 一些人组成团体来制定操作运行规则
 - 小组是如何组件形成的，各种相互作用如何发生；访问策略和访问控制机制；什么人可以有权利查看或拥有哪些数据，当成员加入或离开时怎样做到数据保护。
- 三类团体类型
 - 小型：例如班级家长协会
 - 数字资产转让：例如股票交易
 - 大型：例如转移交易个人健康记录，或者环境数据。

Digital Society: A New World

- From contract preparation and analysis, we now move into
 - Material analysis and legal validation before contract preparation, such analysis can be done by “Watson lawyer”.
 - Contract will be developed as “code” as smart contract and it must have certain regulations.
 - Smart contract must be executable in a flawless manner.
 - Results will be stored in blockchain that can be used for legal evidence.

Digital Society: New Law and Regulation

- Law will be written in “code and data”, and the law will be compatible with the existing law today. Law will be analyzed by Legal Watson for consistency, completeness, and legality.
- Communities such as companies can have their own law with sub-communities, and each will have their own law, all of them written in executable code.
- Individuals will have their own “digital ID” different from traditional ID as their privacy will be of highest priority.

A New Computing Architecture

- Digital society will need new architecture with
 - Smart and autonomous agents;
 - Agent discuss, meet, and trade with other agents via “smart contract” that are legally binding and are automated executed upon asynchronous events;
 - Data and code are stored in blockchain;
 - Software verification, monitored execution, and proper result dissemination are important.

附录 1: Windhover 过渡原则

Windhover 过渡原则

- 所有人都应有平等的主权，对数据、算法、传感器和其他手段的平等和通畅的访问和控制，其独特的生物和行为的身份被定义和确认。
- 所有人都有自主权的自我治理的主权权利，任何个人可以形成自己的分布式自治组织或企业与其他人的生产和分配的资源，货物和服务。

Windhover 过渡原则

- 分布式自治机构（DAO）应：
 - 不断发展，以实现所需的透明度，实现问责制和信任。
 - 不断发展，以减少交易和协调成本。
 - 使用合同和协议，自我执行和自我修复。
 - 保持开放和安全的，所有成员的绩效/活动日志，对DAO实现透明化，鼓励学习和自我修正。
 - 最大限度地减少制裁成本和惩罚，以避免诉讼成本、不利的对策和不必要的社会干扰。

Windhover 过渡原则

- DOAs有权利用实验和参与的新机制实现自我管理、治理、裁决和争议解决，资源和收益分配，市场交换。
- DAOs应当有权发布数字货币和数字资产的交换，反映他们的个人DAOs的价值和利益，这应是自由贸易和交换价值的其他货币。

Windhover 过渡原则

- 所有的人民应该能够为开放的数字身份依靠一个独立的和开放的全球公共资源提供技术支持，治理算法和指标，使个人、团体、事物和过程的真实性的要求可以独立地测试和验证。

Windhover 过渡原则

- 所有的个人和团体对个人资料资产有主权控制权，并有权从一个分布式自治组织转移到另一个独立的组织。没有DAO或其他方不得强迫一个人或团体放弃或共享数据或服务，这侵犯了他们的个人尊严。

尊重信任框架

“尊重信任”框架 (Respect Trust Framework)

- 五个的原则控制身份证和个人数据, 概括为“5个准则 (p)”:
- 1) 承诺 (promise),
- 2) 许可(permission),
- 3) 保护 (protection),
- 4) 可移植性 (portability) 和
- 5) 证明 (proof) 。