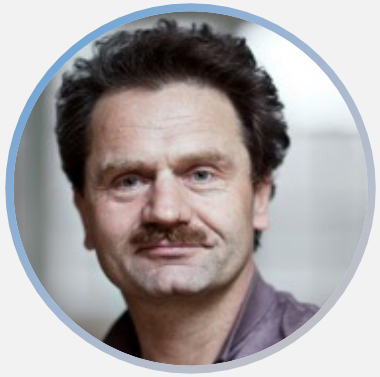
Smart Contracts:
Potential and Reality

Fritz Henglein

U. Copenhagen & Deon Digital

Deep Tech Summit

2021-11-30



Fritz Henglein

Professor of Programming Languages and Systems
University of Copenhagen

Head of Research
Deon Digital AG

Areas of interest

- Programming language technology
- Theoretical computer science (algorithms, semantics, logic)
- Blockchain technology
- Contract management
- Financial technology
- Enterprise systems

Related background

- European Blockchain Consortium (ebcc.eu, CPH), European Blockchain Institute (NRW)
- Steering committee chair, Innovation network for Finance IT (CFIR.dk, until 2018)
- Head of research groups/research projects: Decentralized Systems, Functional High-Performance Computing

Academic background, affiliations, guest positions

TUM
RUTGERS THE STATE UNIVERSITY OF NEW JERSEY
NYU
Universiteit Utrecht
IT University of Copenhagen
CORNELL UNIVERSITY FOUNDED A.D. 1865
UNSW SYDNEY
UNIVERSITY OF OXFORD

What is a contract?

- Enforceable agreement between two or more parties
  - ``Custom law'': Passed by and applied to *particular parties*; enforced by public authorities
- Specification of (future) obligations, permissions and prohibitions regulating the exchange of economically scarce resources
- Properties:
  - Identifiable parties: Required by law (AML, KYC) and for recourse (court action)
  - Capacity to commit:
  - Consideration: Not one-sided exchange of resources (money, goods, assets, services)
  - Confidentiality: By default not disclosed to other parties (unless required by regulation)
- Examples: Sales, services, lease, financial (loan, bond, derivative), insurance, shareholder, mobility, transportation etc.

What about contracts and the economy?

- Corporation as a nexus of contracts (Jensen/Meckling 1976)
  - *It's all about contracts*: Figuring out what to do in the future, committing to it, doing it (and knowing something about what the future brings).
- Standard contracts:
  - Goods, assets, services for money (commercial contracts)
  - Money now for money later (financial contracts)
- Transactional execution is *crucial*:
  - Good: Get asset, give money (successful execution)
  - Okay: Neither get asset nor give money (`successful' abortion)
  - Bad: Get asset, don't give money (contract breach)
  - Bad: Don't get asset, give money (contract breach)
- Economic potential: Digitalization of data, automation of contract execution, guaranteed transactionality
  - Robotic contract managers
  - Transactional resource management systems
  - Require *digitalized contracts*: contracts as code

What is a ``smart contract''?

- Szabo (1994): "A computerized transaction protocol that executes the terms of a contract"
  - What does that mean? (A contract is executed by its participants
- Ethereum (2015): Any program written in the object-oriented programming language Solidity and executed on a blockchain system
  - What do programs have to do with contracts?
    - Do you need to be a programmer to write a contract?
    - Where is the (paper) contract in a smart contract?
  - What do contracts have to do with blockchain systems?
  - What is different about Ethereum-style smart contracts and ordinary programs?
- Smart contract = contract + control + settlement (FH, 2018)

Smart contract = contract + control + settlement

- **Contract** (digital contract): Parties' rules (obligations and permissions)
  - ~ what is written in a paper contract (not how the rules are executed)
  - Both data and *logic* are *formally specified* (no natural language 'residue') in *domain specific language (DSL)*
    - Contract as intelligent data: Can be processed in multiple ways (expected value/price, risk, capacity need, exposure, hedging strategy
- **Control** (contract manager): System that manages contract states
  - Generic: Given any contract submitted to it, it monitors and controls correct contract execution by participants
- **Settlement** (resource managers): Systems that *authoritatively* store resource ownership (money, securities, property rights, etc) and *authoritatively* perform ownership transfers
  - Bank account systems (for transfer of fiat money transfers)
  - Security depositories (for transfer of security ownership)
  - Crypto asset registries (for transfer of blockchain tokens and cryptocurrencies)
  - Danish bicycle registry (for transfer of bicycle ownership)
  - Private parking spot registry (for renting private parking spots)
  - European industrial and art design registry (for registering, leasing and selling intellectual property rights
  - ...

What is a blockchain/distributed ledger system?

A distributed computer system characterized by

- organizational and technical **decentralization**;
- **tamper-proof recording** of events and their **evidence**;
- guaranteed **resource preservation** and **credit limit** enforcement;
- high **consistency** of information across all nodes (single source of truth)
- high **availability** (individual nodes may go down, but whole system remains operational)

What do smart contracts have to do with decentralized systems such as BC/DLT-based systems?

- Ab initio: Nothing
  - Ethereum-style smart contracts could run on bank account system
- In practice: A lot
  - Term ``smart contract'' is a viral meme – it associates with (Ethereum-style) blockchain systems
- Connection:
  - Contracts are between sovereign parties
  - Centralized systems interpose a controlling intermediary
  - Decentralized systems eliminate the intermediary
    - Participation of equals

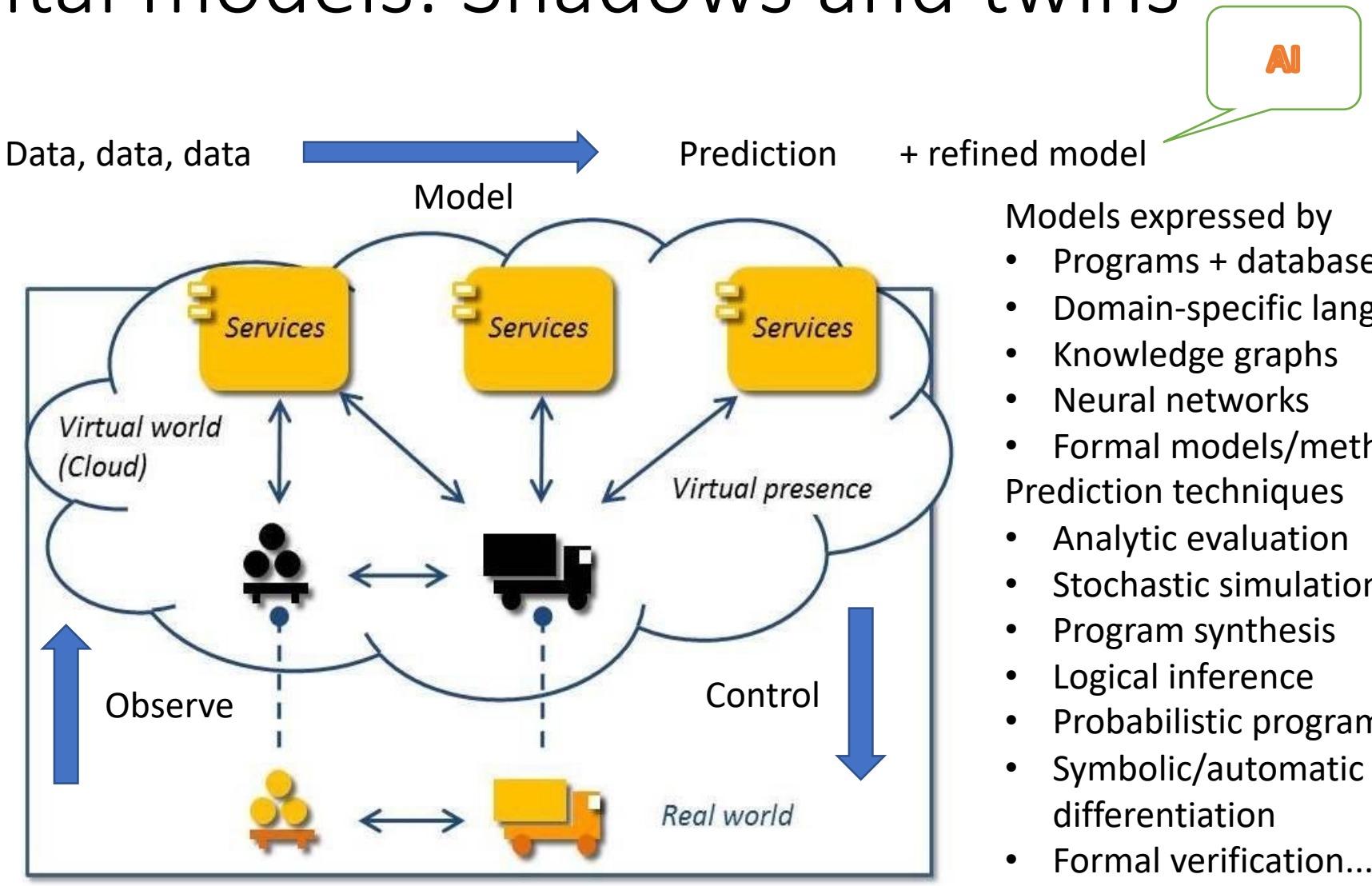
Decentralized systems applications are here

- Trade finance
- Logistics (e.g. TradeLens)
- Track and trace (Everledger, Walmart, CoffeeChain)
- Health care (Healthchain)
- Remittance (cryptocurrencies, stable coins)
- Privately issued synthetic assets (cryptocurrencies)
- Decentralized finance (automated AMs, automated LPs, automated exchanges)
- License management (NFTs)
- Identity management (e.g. Sovrin)
- Debt instrument/financial markets platform (Dromaius/JP Morgan, Deon Digital/R3 Corda)
- Examples: Secure T&T. Smart Financial Instruments

Circular economy

- Many cooperating *and* competing **agents**
  - Decentralized governance
  - No Big Brother required or intended
- Transformation, storage and transportation of **natural**, **biological** and **synthetic resources**
  - Where do they come from?
  - What is in them?
  - Where are they going?
- **Circular resource economy**
  - Nothing is ever ``produced''
  - Nothing is ever ``discarded''
- ... and how to finance it?

Digital models: Shadows and twins



Models expressed by

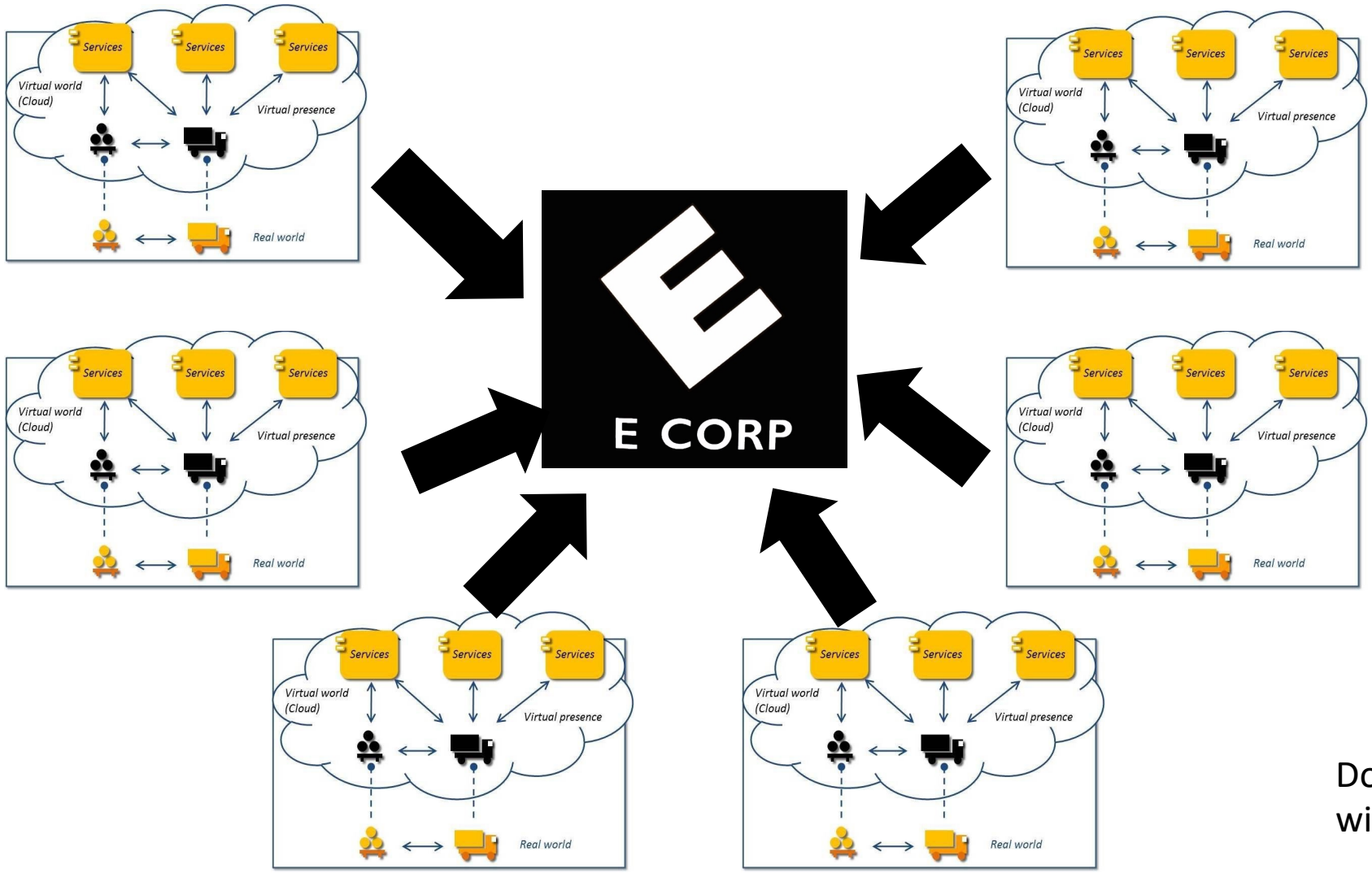
- Programs + databases
- Domain-specific languages
- Knowledge graphs
- Neural networks
- Formal models/methods

Prediction techniques

- Analytic evaluation
- Stochastic simulation
- Program synthesis
- Logical inference
- Probabilistic programming
- Symbolic/automatic differentiation
- Formal verification...

Dalmolen, Cornelisse, Moonen, Stoter, Stoter: Cargo's digital shadow: a blueprint to enable a cargo centric information architecture

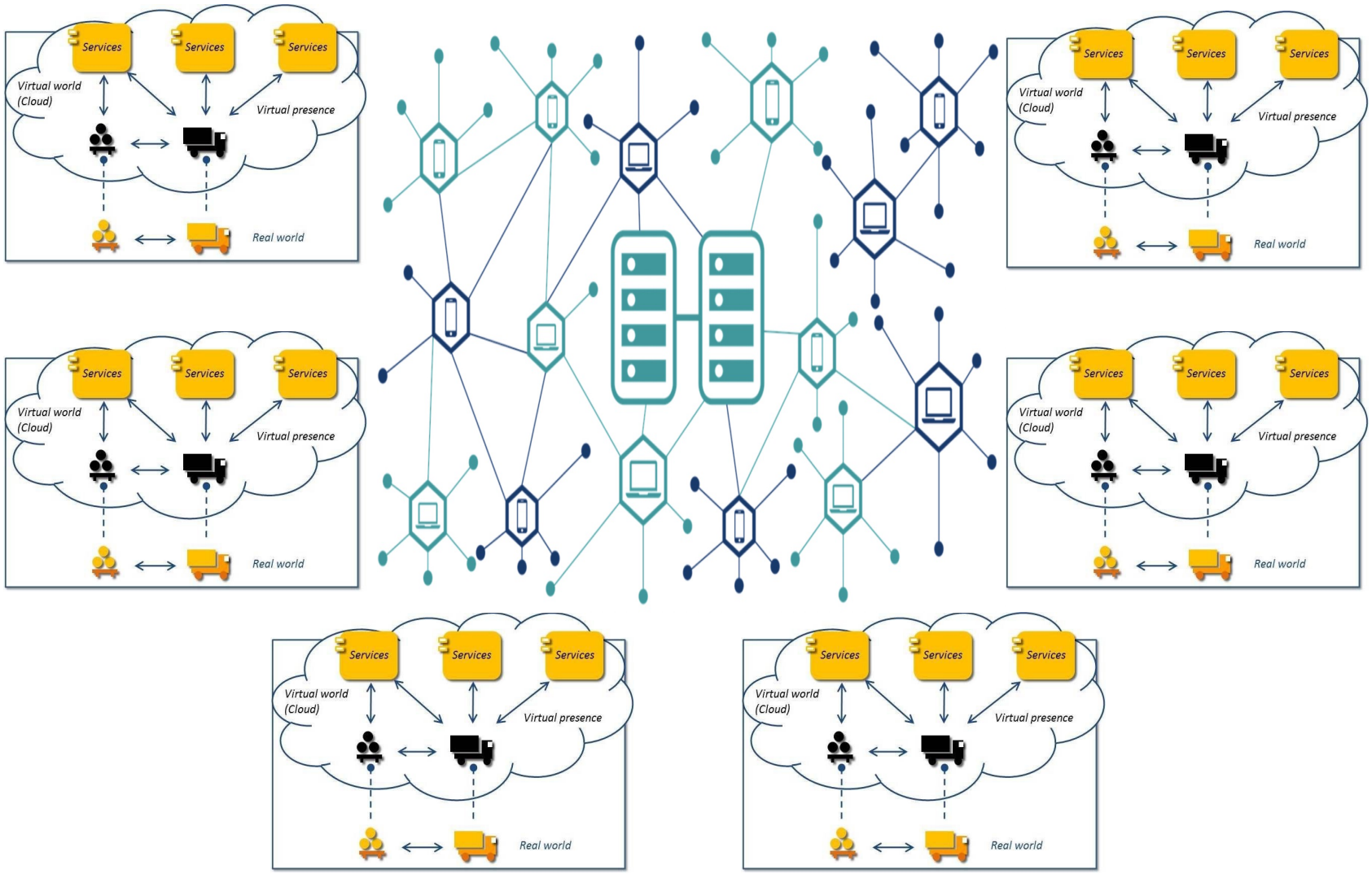
Digital cloud: Centralized governance



Share your data and your models with a **trusted/privileged** platform provider

Does **everybody** trust E Corp with **their data and their models**?

Digital sky: Decentralized goverance



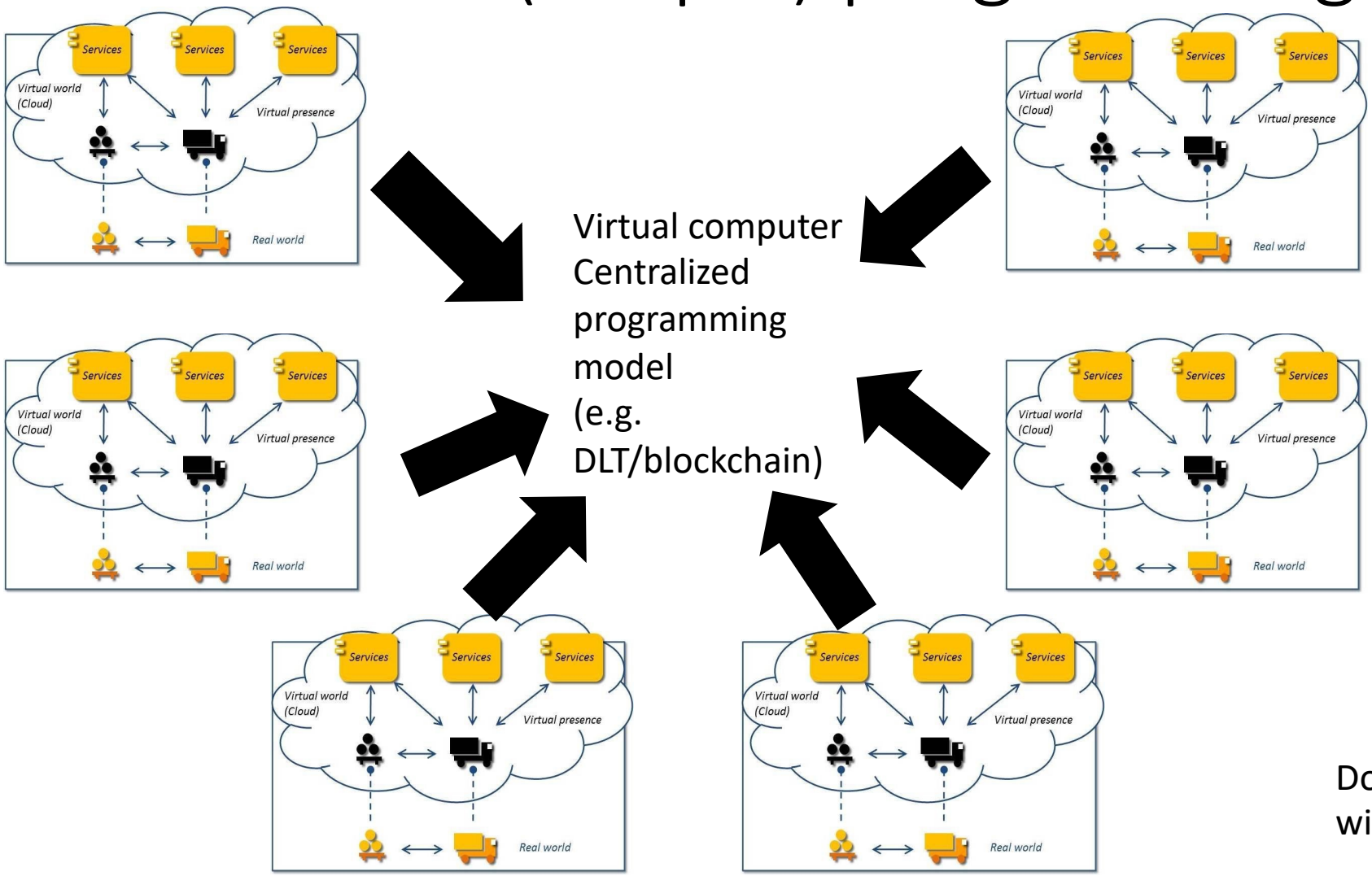
Structured peer-to-peer computer networks

- No single point of control
- Network behaves like single computer
- Blockchain/distributed ledger technology

Cooperative systems

- Tamper-proof recording
- Guarantee against digital forging
- Smart contracts for guaranteed fair exchanges
- Secure multipart computation for secure data sharing

Digital sky: Decentralized governance, centralized (simple) programming model



Share your data and your models with a **trusted/privileged** platform provider

Does **everybody** trust E Corp with **their data and their models**?

Deep T&T for (bio)materials

Project CoffeeChain. Partners: Cowi, Larsen Kaffe, UCPH (DIKU, IGN), Chalmers U., IT U. (2018-2021)

Why blockchain for circular economy?

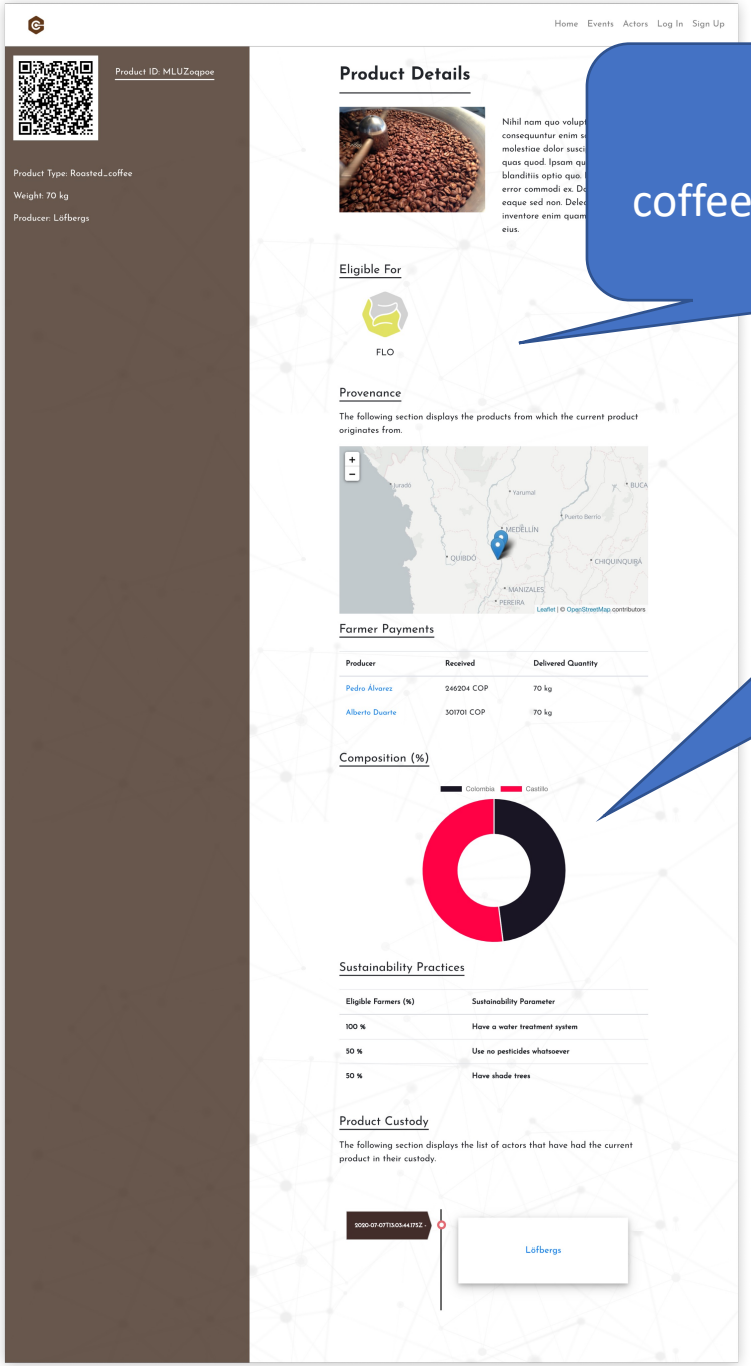
- **Decentralization** → Information symmetry: No single actor controls the data (and thus the supply chain)
  - Instead ofhaving de facto/appointed controlling/privileged party (cloud/system provider)
- **Tamper-proof recording** → Trustworthy and efficient provenance of products *(materials, goods, food, etc.)*
- **Self-sovereign identity management** → Digital signatures, privacy
- **Distributed consensus** → Guaranteed consistency of shared data across all parties (no reconciliation necessary)
- **Secure resource management** → Guaranteed prevention of digital certificate forging
  - Cannot produce more certified products without consuming at least as many certified materials

Benefits of trustworthy Deep T&T

- **Trustworthy product provenance** → safety, regulatory compliance, price differentiation, incentivization to produce sustainably
- **High automation** → low operational cost, inclusion of small producers, sustainability
- **Secure contracting** → payment vs. delivery, escrow, collateralized credit
- **Decentralization** → open platform, self-sovereign identity, no private (government) platform owner/data aggregator, secure trade, tamper-proof evidence.

CoffeeChain: Status

- Implemented:
  - Ethereum (Solidity)
  - DBMS (MySql)
  - Responsive webapp (React.js)
- Track & trace:
  - Cherry to cup
  - Fungible and nonfungible resources
  - Certification f. sustainability
  - Packing/unpacking
  - Tracing components in products
- Planned:
  - Streaming data source integration
  - Real-time derived information



Try it:
coffeechain.herokuapp.com

And try the coffee -- now!

Green Finance

Require 20-30 year investment horizon

Require > EUR 2.500 bn/year Investment

Problem solved?

Hav
inve
hor

Barrier!

Green bonds -- efficiently?
ESG scoring -- trustworthy?

Have > EUR 2.500 bn/year to invest

"$3-7 trn/year for many years to come", Philip Hildebrand, vice chairman of BlackRock, World Economic Forum, 2021

Green Finance: Smart Green Bonds

- Green bond
  - **Bespoke:** Specially designed for each project (e.g. particular to windmill farm)
  - Integrated environmental, sustainability and governance (ESG) conditions (e.g. certified windmill-generated electricity from certified windmills, no double spend guarantees [greenwashing])
  - **Risk sharing** (e.g. coupon payments depend on wind energy produced)
  - **Unusual derivative**: Depend on observations other than interest rates and stock prices
- Challenges:
  - Efficient admission. Bespoke: too costly, if one at a time.
  - Efficient life-cycling (payments, corporate actions, etc). Bespoke: No existing software in standard markets
- Opportunity: Demand + no effective and efficient solutions
  - Pledges, momentum (DKK 350 bn by 2030 pledged by Danish pension funds)

Smart financial instruments

- **Smart financial instrument**:
  - money-now-for-money-later *contract*
  - expressed in domain-specific language (DSL)
    - For and used by financial engineers
    - Mechanized mathematical semantics
    - Analyzable (security/fairness, pricing, volatility, extreme scenarios)
  - Applicable to other domains (intermodal mobility, logistics, insurance, etc)

```
data Contract b where
   Fail    :: Contract b
   NoEvent :: b -> Contract b
   Event   :: Event b -> Contract b
   Then    :: Contract a -> (a -> Contract b) -> Contract b
   Par     :: Contract a -> Contract b -> Contract (a, b)
   Alt     :: Contract b -> Contract b -> Contract b
```

Smart financial instruments: Architecture

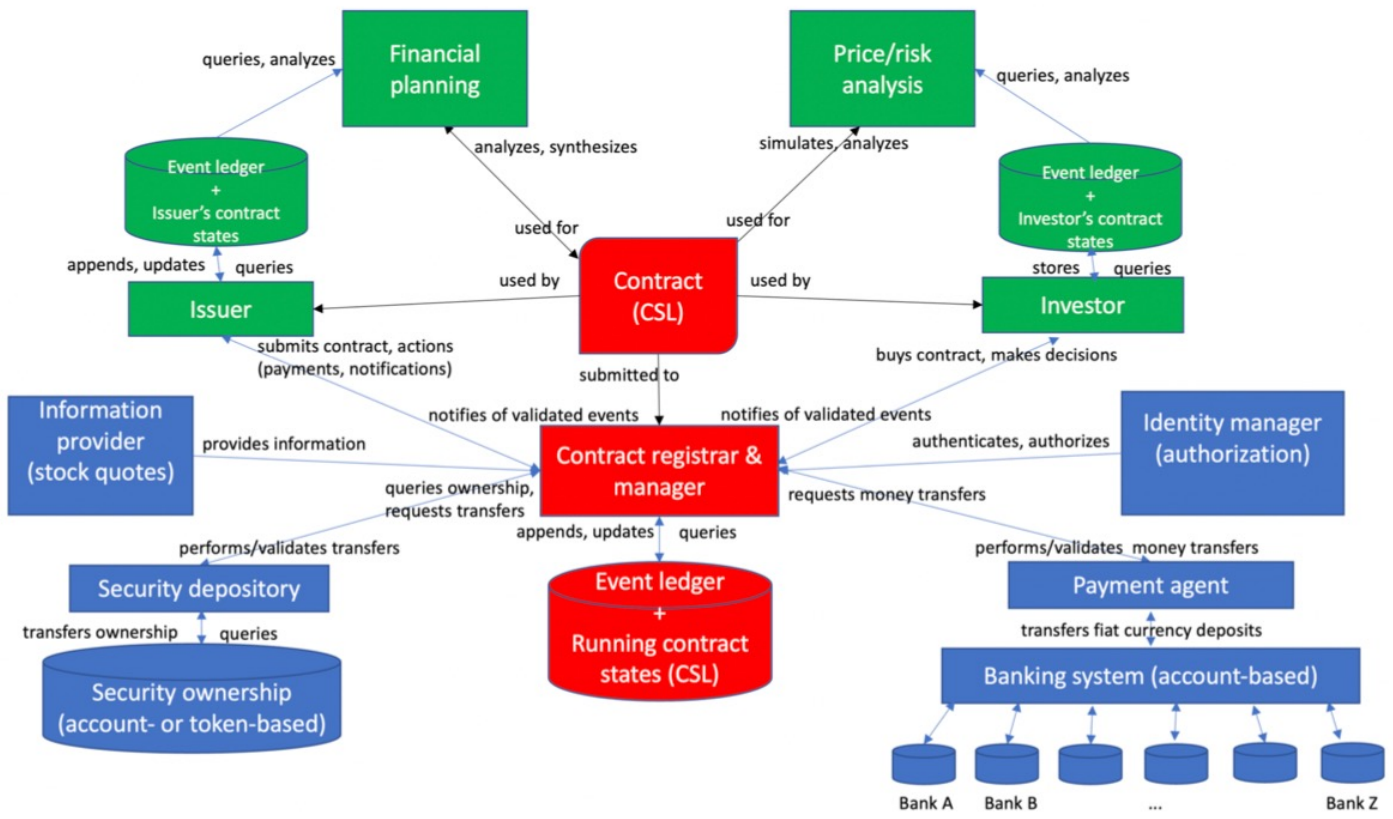


Figure 1: DLT platform architecture, core components. (Transaction manager not shown.)

Smart financial instruments

- **Smart financial instrument**:
  - money-now-for-money-later contract
  - expressed in domain-specific language (DSL)
    - For and used by financial engineers
    - Analyzable (security/fairness, pricing, volatility, extreme scenarios)

```
data Contract b where
   Fail    :: Contract b
   NoEvent :: b -> Contract b
   Event   :: Event b -> Contract b
   Then    :: Contract a -> (a -> Contract b) -> Contract b
   Par     :: Contract a -> Contract b -> Contract (a, b)
   Alt     :: Contract b -> Contract b -> Contract b
```

Smart financial instruments: Example

```
zeroCouponBond issuer currency notional maturityDate bdc =
  Event Transfer
  `suchthat`
  (\t -> sender t == issuer
      && (currency.resource) == currency
      && (money.resource) == notional
      && date t == bcd maturityDate)
```

CSL2 (under development).
See deondigital.com for Deon Digital CSL (deployed in products)

Architecture highlights

- **Real-time**: 5 second settlement (latency) instead of 200.000 seconds
- **High throughput**: 1+ million transactions/second per server (including settlement, persisting, crash-fault tolerance, cryptographic security)
- **Scale out, security and privacy**:
  - Contract managers independent: n servers -> O(n/log n) * 1-server transaction throughput
  - One private channel per contract
  - High-throughput resource managers (account-based currencies/fungible tokens, netting optimization)
- How? (Avoiding global consensus as in current-generation level-1 blockchain/DL-systems)

From 200.000 seconds to 5 seconds: So?

- **Direct control and contracting**: buyer-to-seller, no custodian/broker/CCP needed
  - No counterparty risk
  - No settlement risk
  - Low capitalization requirements for security registristry and trade platform provider
- **Light(er)-weight regulation** does not require intermediaries: EU MiCA (crypto assets), EU DLT pilot for MiFiD II (financials instruments), Swiss DLT Effekten
  - Lower capital requirements for security registry and trade platform provider
  - DK license -> EU passport
- **Register and trade anything**, down to 25 Eurocent tokens (peer-to-peer parking, Power-to-X-certified electricity chargers, <your business/NGO idea here>

Summary

- Digitalized contracts: *data* and *logic* as code
- Smart contracts/contract managers: Contracts monitored and controlled and transactionally executed on trustworthy system
- Resource managers: Efficient transactional ownership and transfer management of economic resources
- Decentralized systems: No choke point, no controlling intermediary
  - Supply chain dominator, cloud service provider, government-controlled system, biggest competitor, ...
- Lots of economic application potential, rising number of applications
  - Financial contracts, trade finance, logistics, crowd funding, secure track and trace, provable sustainability, ...