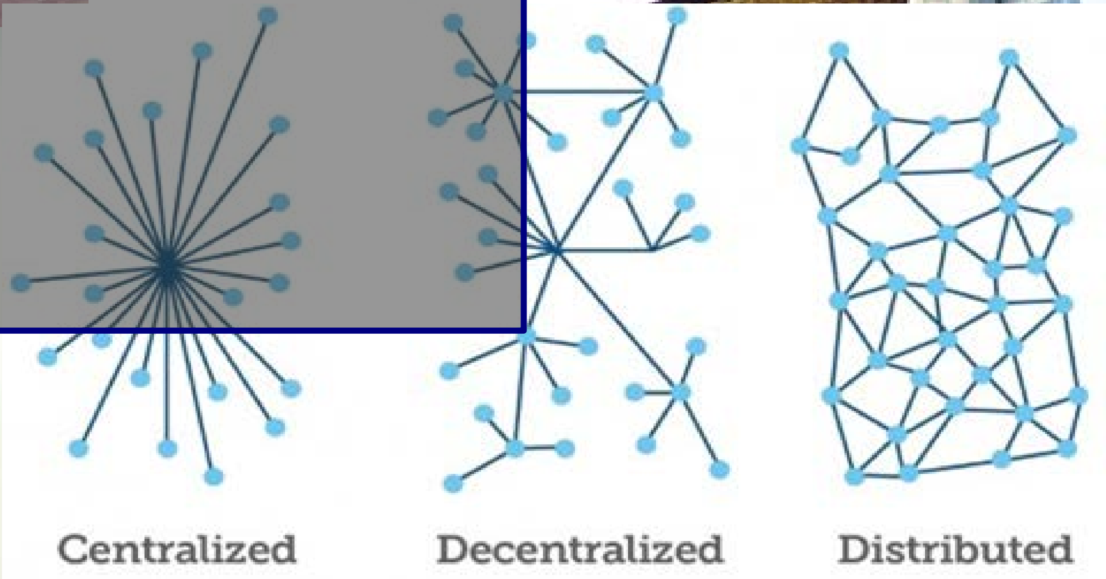
Artificial Intelligence in Industry and Finance (3rd European COST Conference on Mathematics for Industry in Switzerland)

September 6, 2018, 9:00-17:30 - ZHAW Winterthur, Technikumstrasse 71, 8401 Winterthur

Blockchain and Financial Risk Reporting: design principles and formal reasoning

Nikos TRIANTAFYLLOU, UAegean ✓
Katerina KSYSTRA, UAegean
Petros STEFANEAS, NTUA
Petros KAVASSALIS, UAegean

✉ pkavassalis@atlantis-group.gr



RegTech and Financial Reporting

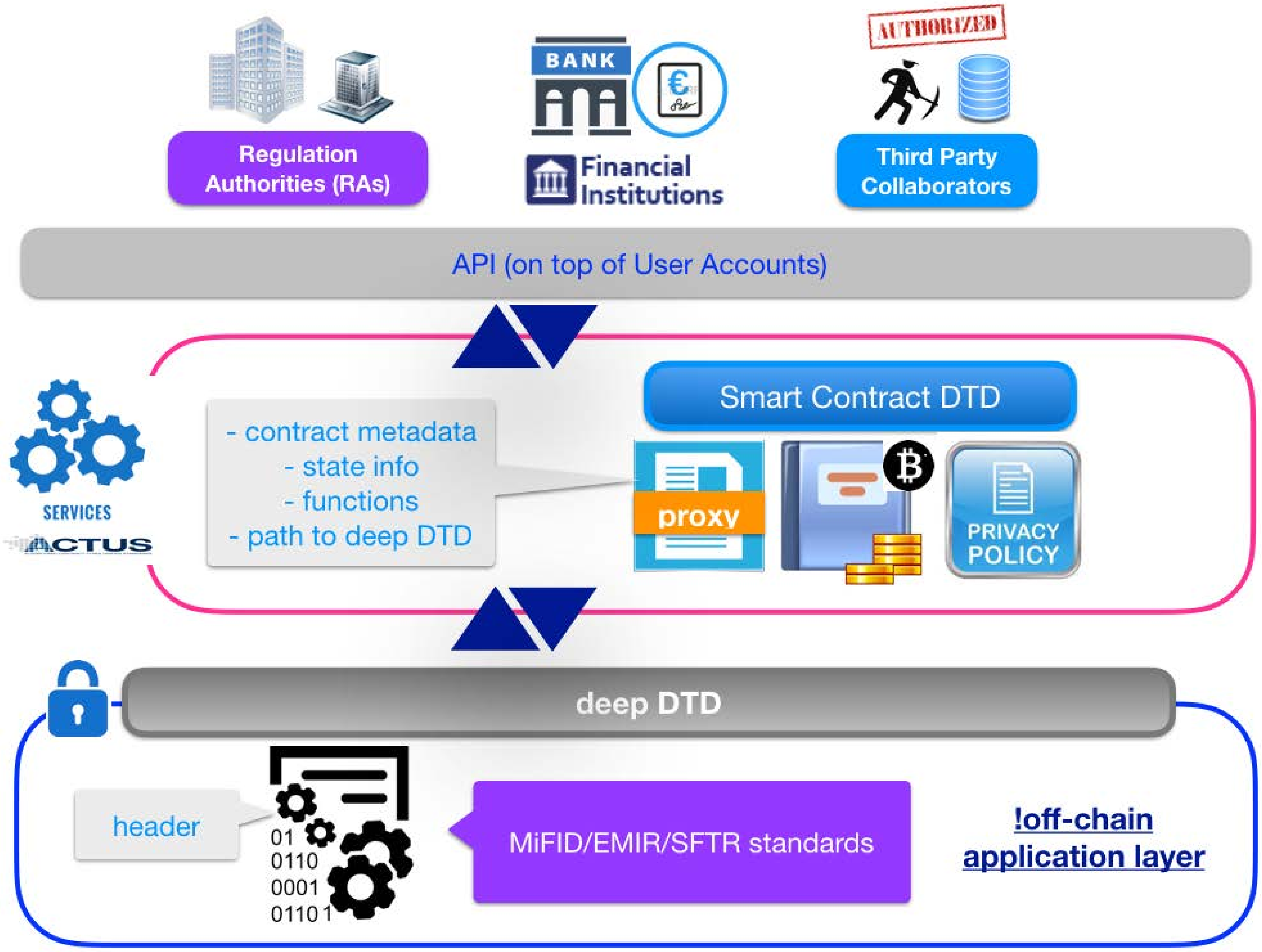
- Two years ago, one of the authors of this paper, and H. Stieber (EC), W. Breyman (ZHAW), K. Saxton (KS Strategic), F. Gross (ECB), have proposed a **RegTech approach to the reporting of financial transactions** that allows for the "on-the-fly" assessment of the financial risk (Kavassalis et al, 2017, The Journal of Financial Risk). It is about (simply put):

  - Engineering a document that complements any financial contract, to keep track of it, and establishing it onto RegTech authoritative blockchain ledger
  - Assisting regulators, governments and the "society at large", in overshighting the global financial system and act long before a full-blown crisis has time to develop

RegTech approach to financial reporting: basic components and architecture

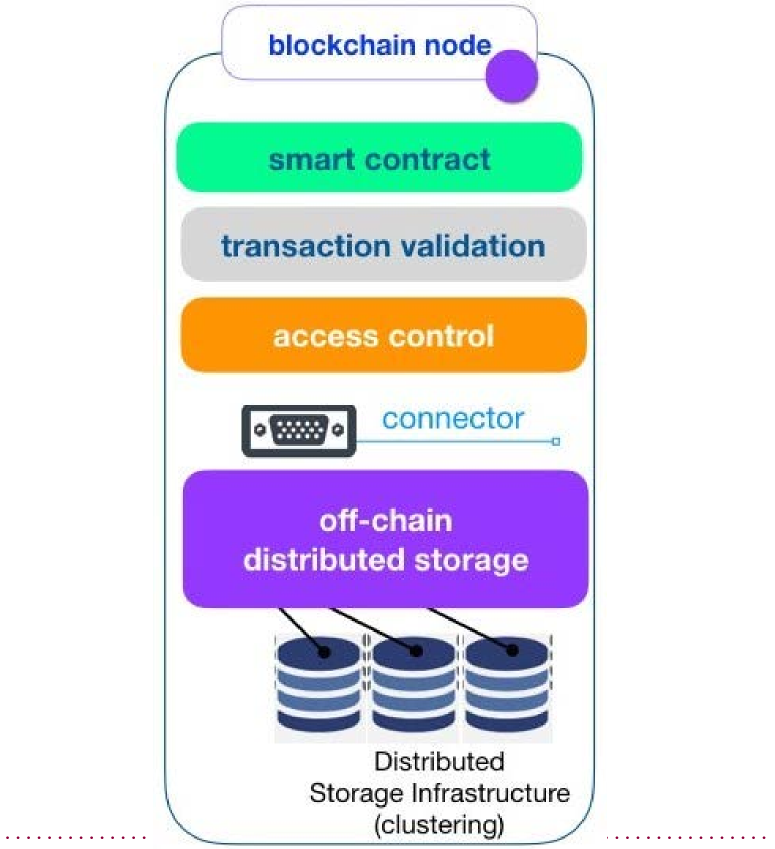
- ⌘ **Methods and technologies**: Distributed computing and decentralised data management technologies such as distributed ledgers (DL), distributed storage, algorithmic financial contract standards (ACTUS), document engineering methods and techniques, formal reasoning.

- ⌘ **Architecture**: Inspired from the concept of the Internet “bearer service” and its capacity to span over existing and future technological systems and substrates (Kavassalis et al., 2000, Clark, 1988). A RegTech bearer service generates and maintains a “digital doppelgänger” for every financial contract in the form of Dynamic Transaction Documents (DTDs), i.e. a standardised “data facility” automatically making important contract data from the transaction counterparties available to relevant authorities (and to their collaborators).
  - DTD is a smart contract that publishes (under specific access policy rules) and processes (by interacting with external ACTUS deployments) real-time financial information, to deliver actual and expected cash-flow aggregation information (and other inputs from economic analysis); transaction and risk information is transferred directly, seamlessly and trustly from the IT Systems of the FIs to regulators line-of-sight.



A DTD has a two-fold structure:

1. a core DTD: a smart contract living in a permissioned blockchain
2. a deep DTD: the transaction report stored off-ledger


blockchain node
smart contract
transaction validation
access control
connector
off-chain distributed storage
Distributed Storage Infrastructure (clustering)

(Two years later, DLT (Distributed Ledger Technology) is largely considered as one of the driving forces for the evolution of the financial system)

RegTech and financial risk: stylized facts (1)

- **Financial Stability Board (2017)**: “Across a range of economic functions, financial institutions are investigating applications for DLT – for cross-border interbank payments, credit provision, capital raising and for digital clearing and settlement… Other innovations are seeking to change how information and services are provided to the market. Smart contracts can be used to automate transactions and business processes, thus reducing transaction costs. For instance, estimates suggest that mortgage borrowers in the US and European markets could potentially save $480 to $960 per loan and banks would be able to reduce costs in the range of $3 billion to $11 billion annually by lowering processing costs in the mortgage origination process… Throughout the full spectrum of financial services, internal auditors, regulators and supervisors, for example, to **reduce the costs of regulatory reporting (“RegTech”)** or to detect risks early on, can also use FinTech…”
- **C. Long, former chairman & president at Symbiont.io (2017)**: “... The financial system has many forms of leverage that don’t show up on the nancial statements of individual nancial institutions, but exist in the financial system as a whole — making it riskier. Rehypothecation is just one flavor… Multiple parties report that they own the very same asset… DLT could give regulators the ability to monitor markets in real-time, providing transparency via a “read-only” node on a DLT network. This would give regulators transparency regarding counterparty relationships and systemic leverage in real-time, and would automate the regulatory reporting required of regulated companies…”

RegTech and financial risk: stylized facts (2)

- ⌘ **J. Christopher Giancarlo, US Commodity Futures Trading Commission | CFTC (2016)**: “...I was on Wall Street, serving as a senior executive of one of the world’s major trading platforms for credit default swaps (CDS), then the epicenter of systemic risk… . Panic was in the air and tension was on our broking floor trying to maintain orderly markets... trading conditions were deteriorating by the hour. It was clear **that the regulator had little means, short of telephone calls, to read all the danger signals that the CDS markets were broadcasting**… Now, let’s fast forward to today. It is seven and a half years after the financial crisis and **global regulators still do not have full visibility into the swaps trading portfolios of major financial institutions**... CFTC data still does not provide a complete picture of global swaps trading. In part, it is because global regulators have not harmonized global reporting protocols and data fields across international jurisdictions. It is also because of the practical impossibility of a single national regulator collecting sufficient quality data for both cleared and uncleared swaps to recreate a real-time ledger of the highly complex, global swaps trading portfolios of all market participants. Fortunately, **emerging distributed ledger technology, what I will call “DLT” or “blockchain,” may address this crucial need**… Blockchain may finally give to regulators transparency… DLT offers the promise in allowing U.S. government overseers to transcend the fragmented regulatory structure by providing reference to a single, verified record of all financial transactions across regulated markets…”.

RegTech and financial risk: stylized facts (3)

- ⌘ **DTCC (04.2016)**: “Seven firms announced today the successful test of blockchain technology and smart contracts to manage post-trade lifecycle events for standard North American single name (CDS)... The initiative demonstrated that the complex events inherent to CDS, including payments, amendments, novations and compressions, can be efficiently managed on a blockchain in a permissioned, distributed, peer-to-peer network..”. The test has generated “**smart contracts from CDS trade confirmations creating a synchronized, distributed golden record on the network**. Embedded in those smart contracts were economic terms, as well as computational logic to manage permissions and event processing. The project also demonstrated the transparency which **could be made available to regulators in real time, including individual trade details, counterparty risk metrics and systemic exposure to each reference entity**…”.
- ⌘ **Axoni (2018)**: Axoni's suite of enterprise software supports integration of blockchain infrastructure into the FI’s IT systems in place (**shares** and **synchronizes** data across applications and systems by using **smart contracts** to encode data, calculations, and event-driven activity on the blockchain, and **provides regulatory reporting**).
- ⌘ **New EU Regulation (2020) requiring reporting to Trade Repositories**: SFTR (Securities Financing Transaction Regulation) goes live, with **SFTR reporting** planned to start in **Q1 2020** (SFTR reporting follows on previous reporting regulations: EMIR (covers OTC and exchange-traded derivatives) and MiFID II (regulates derivatives and cash financial instruments while focusing on transparency and market abuse).

It is tempting to think that the concept of DTD becomes very topical...

- A DLT-enabled DTD (Dynamic Transaction Document) may **overarch the different** reporting methodologies, standards and regional/national reporting frameworks, to create a minimal data facility and eventually provide “a **real-time ledger** of the highly complex, global swaps trading portfolios of all market participants”.
  - (In Internet terms, to use a metaphor) DTD might look like the equivalent of IP layer residing on top of the powerful technology substrates of Internet Service Providers (ISPs).

- **How?** What are the **primary features** of a DTD?
  - Stores a “digital doppelgänger” for every financial contract (i.e. a coded replication of all relevant features of the actual contract on which a FI needs to report) to provide a **unique algorithmic representation of the current and expected behaviour of the underlying contract**; essentially, it would track and monitor the evolution path of the underlying contract during its whole life-cycle, at each stage providing updated quantitative information, i.e cash-flows).
  - Allows for **aggregate insights to recognize counterparty trading exposures** indicating potential financial risks and eventual shortcomings in market activity.

Let’s be clear enough...

e the essential contribution of DTD? “Stop financial crises before they start”!

ve the capability of the regulation authorities to timely collect accurate reporting information, on a **act per contract level** for **all financial institutions**.

de **standard risk metrics for particular or aggregated financial instruments and FIs** (eventually

or in quasi-real time the relative positions of FIs and their inter-dependencies (exposures).

ify “bad” contracts that eventually impose risks, to diagnose financial market failures early...

use DTD? **Only** regulators? Not only regulators, but also the “society at large”!

rized collaborators of Regulation Authorities

rsities, Research and competent NGOs

vision that the blockchain and DTD will cause **the number of controlling entities of the system to proliferate?**

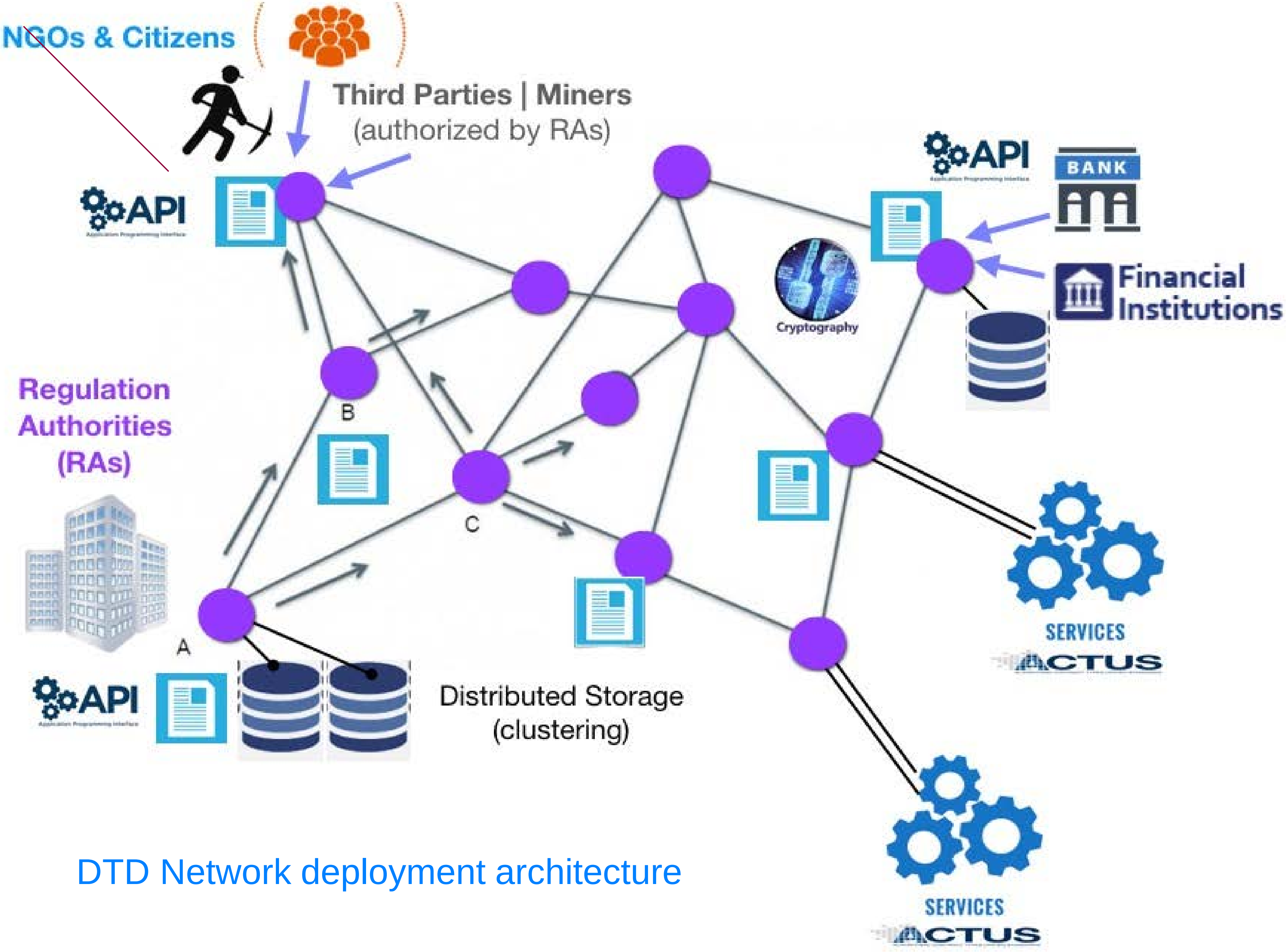
rhaps similarly to what happened with the advent of ECNs (electronic communication networks); in ECN caused the number of trading venues to increase rapidly in number, in all continents (C. Long, ...

DTD is a public good! Let’s design it accordingly...

1. Regulation is needed!
    - DTD cannot be expected to be provided by FIs left to themselves, creating a need for specific regulation that will initiate the new construct.
2. The first problem to solve: **economic design** of DTD as public good
    - We need a mechanism design theory for DTD, i.e. identify the institutional properties of DTD that make it economically efficient and successful.
3. The second problem to solve: **derive design principles for a robust evolvable network** supporting DTD creation, diffusion and sharing (in conditions of data privacy and non-disclosure of sensitive financial data) based on the combined use of:
    - Blockchain and smart contracts
    - Financial analytics intelligence (ACTUS standards)
    - Formal reasoning and methods for precise design

Design principles for “DTD as public good”

1. **Implement a DLT-based layer of financial and risk reporting functionality** that integrates smart contract processes with an ACTUS contract types server, and support from an off-chain storage infrastructure (core functionality)
2. Create **APIs to financial institutions’ IT Systems** (counterparty functionality)
3. Design a **blockchain-enabled distributed access control policy** to DTD data (sharing functionality)
4. Provide **formal mechanisms for data validation**, to ensure that the financial information inserted from the FIs in the system is accurate (data validation functionality)



DTD Network deployment architecture

TKSK [2018]

Progress in architecture design and Proof of Concept

- Several contributions to prove the **feasibility of the concep**t and the **successful integration with ACTUS standards**
  - M Sel et al: Use of Ethereum smart contract to implement a basic model of a bond (modelled after an ACTUS “Principal at Maturity” or “PAM” contract type) and an interest rate swap (modelled after an ACTUS “SWAP” contract type).
  - P. Kavassalis et al: Create a DLT-base reporting demonstrator for a simple economy consisting of three interrelated banks and a regulatory authority (permissioned blockchain).
  - Work in progress...

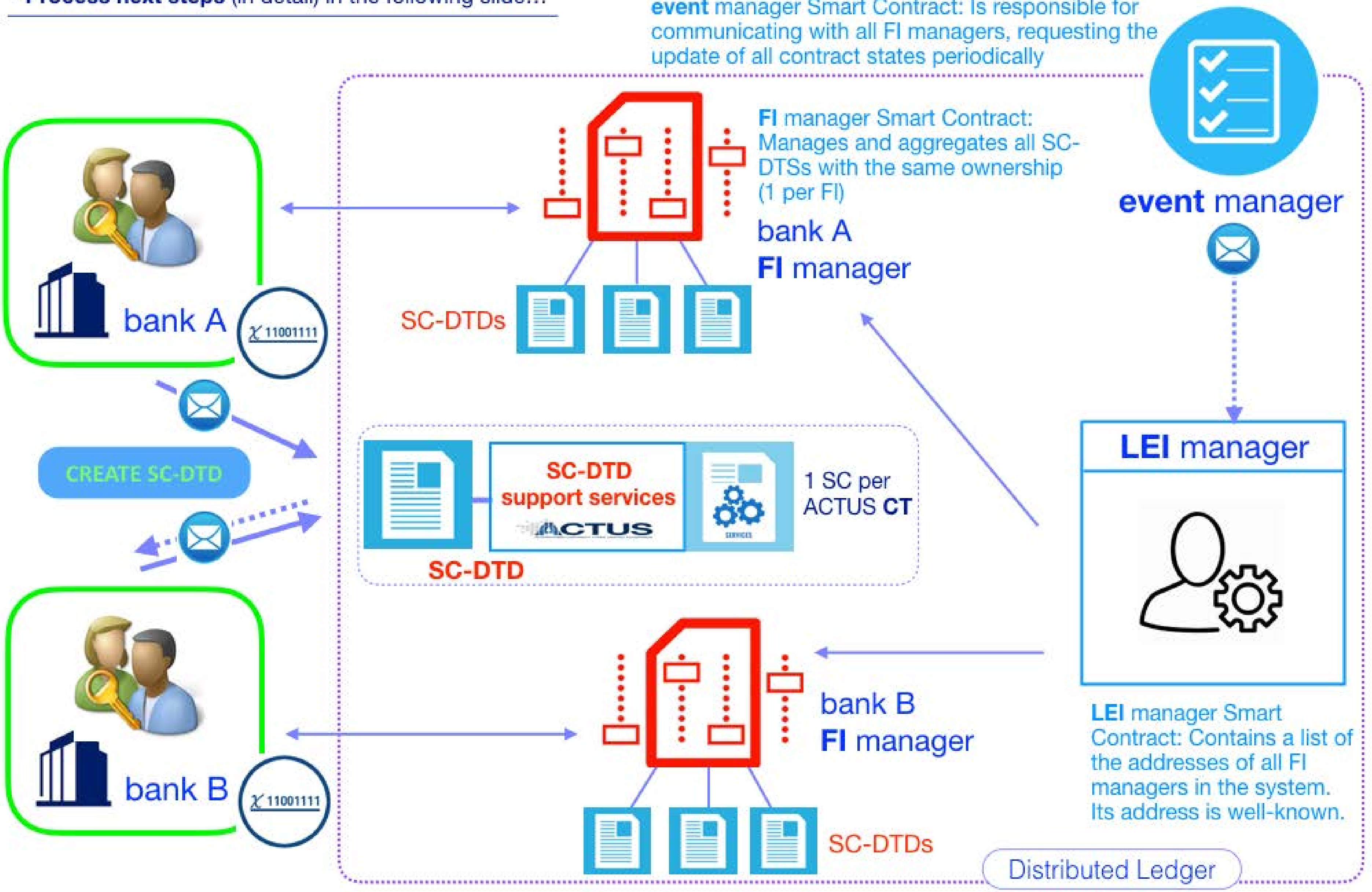
- However, the immutable nature of the blockchain may guarantees the safety from tampering and revision of the data and contracts therein, but displays zero/minimal tolerance for design flaws or logical bugs!
  - Formal methods can provide solutions for such problems in a rigorous way
    - Mathematically based/computer aided techniques for reasoning about complex systems
    - Computer handles tedious computations
    - Humans bring in intuition and domain knowledge

- Bank A and Bank B **jointly** report a financial transaction made through their connected IT systems.
- That means: Banks A and B **jointly sign the report** by using their DL accounts and **transfer access rights** to the competent Regulation Authority(ies).
(*) Part of the reported information will become instantly public according to the reporting rules.
- The signed transaction is **broadcast to the DL** to be **validated** and **recorded** in the next update.
- **Process next steps** (in detail) in the following slide…

Develop a formal framework for reasoning about smart contracts

1. Reasoning about smart contract business logic (architecture design through formal specifications)
2. Implementing business logic correctly (formal verification).

DTD Network: internal components



event manager Smart Contract: Is responsible for communicating with all FI managers, requesting the update of all contract states periodically

FI manager Smart Contract: Manages and aggregates all SC-DTSs with the same ownership (1 per FI)

LEI manager Smart Contract: Contains a list of the addresses of all FI managers in the system. Its address is well-known.

TKSK [2018]

Case: Minimum Safety Property

It is not possible to have a “confirmed” contract in DTD Network
without the the approval of all involved parties first
(Data Validation)

Core Ontology for blockchains

- We can identify in a Blockchain system the following basic structures;
  - Subject
    - The elements of the sort Subject, are used to denote the users of the blockchain.
  - Object
    - Objects denote the entities on which the actions of the system are applied.
  - Actions
    - The Action domain contains all the actions permitted in a blockchain system
    - The actions defined in our system are the following: createAccount, createContract, updateContract, validateContract, getReport
  - Transactions
    - The elements of the Transaction domain denote a desire or a request by the subject to execute an action on the object of the transaction.

State Transition and blockchain (1)

- The information contained within a Blockchain constantly changes! To address this, we define a new structure, called State, which represents the state space of the blockchain system.
  - In fact, a blockchain can thus be thought of as a State Transition system, where:
    - Each state consists: of the status of the core entities of the system
      Each state transition function: takes as input a previous state of the system and a transaction and gives as output a new state.

- A new constant is declared, init : → State, which denotes the initial state of the system (i.e. it represents the genesis block of the blockchain).

- Three constructor functions are declared, which define how a new state of the system can be derived by a previous one, sendTransaction, validateBlock and Tick.

State Transition and blockchain (2)

- ⌘ Core functions
  - sendTransaction: State Transaction → State, denotes that a new transaction is sent to the system.
  - validateBlock: State Transaction Transaction → State, denotes that a set of received transactions were considered as valid and their actions took effect altering the state of the blockchain (i.e. represents the mining of a new block in the blockchain).
  - Tick: State → State, denotes the passing of time and is required because the information retrieved by a smart contract may change depending on this.

- ⌘ More functions:
  - pendingTransactions, which denotes the transactions submitted to the system but are not yet verified, i.e. the transactions which are pending validation.
  - objects, which given an element of the sort State returns a set of object sorted elements and denotes the objects that belong to the blockchain at the given state of the system.

Network Specification: Smart Contract

- A smart contract is represented by a subsort of the sort Object.

- We define the following types of smart contracts (sc):
  - LEIManager: register and allow the retrieval of all users in the system (regulators and financial institutions
  - FIManager: acts as a proxy for a financial institution on the system. Manage and aggregate all smart contracts in the system with the same ownership.
  - Smart Contract DTD (SC-DTD): represents a single real world financial transaction.

- Stateful

- Each such sort (sc) defines a set of “observation” functions:
  - e.g. for DTD : validator, validated, getReport etc.

Network Specification: Transitions

- We define the following transitions:
  - createFIManager: State String String → State, takes as input a state of the system and two Strings, denoting the id of the new FIManager and the id of the registered user who creates the FIManager, and produces a new state of the system.
  - createActuscontract: State ActusContract String String → State, takes as input a state of the system, an Actus contract and two Strings and produces a new state of the system. The first input String corresponds to the id of the user responsible for creating the contract and submitting the contract data. The second input String denotes the id of the second involved party referred to the contract.
  - validate: State ActusContract String → State, takes as input an ActusContract and a String denoting the id of some party, and sets the id of the validator of the contract.
  - Tick: State → State, denotes the advancing of time in the system.

Reasoning with algebraic specifications & formal verification

⌘ Reasoning with algebraic specifications

- Algebraic specification method is considered as one of the major formal methods.
- Systems are specified/designed based on algebraic modeling.
- The specifications/designs are tested/verified against requirements using algebraic techniques.
- The behavior of systems can be nicely modeled by algebras.
- **CafeOBJ** is an algebraic specification language.

⌘ Formal verification: “It is not possible to have a “confirmed” contract in DTD Network without the the approval of all involved parties first”

- Using the OTS/CafeOBJ approach, we successfully verified that the specification satisfies the desired system property.
- The full specification of the proposed system and the proofs can be found at CafeOBJ@NTUA [https://cafeobjntua.wordpress.com/].

Future directions

- Distributed access control policies verification
- Sharing of information
- Verification of SC implementation
- Scalability (golden ratio)

/thanks!