Designing **Smart Contracts** for Automating Cross-Organizational Collaboration For Blockchain-Tech

Alex Norta, PhD.,
Department of Informatics, TTU.ee
Tallinn, Estonia
Agenda

- Introduction & DIY Blockchain/Bitcoin learning
- Current state in blockchain-tech/crypto-currency
  - Gap and research question
- Business-collaboration model
  - Master/client- vs. P2P-collaboration
  - Detailed collaboration model
- eSourcing Markup Language (eSML)
- Complete lifecycle for smart-contract management
  - Setup
  - Rollout of an ad-hoc decentralized governance infrastructure
  - Disrupting and calming rollbacks for conflict management
  - Termination
- Conclusion and future work
Introduction

Many smart-contracting solutions emerge:

- **Digital anarchy** is coming
- **UltraCoins** to eliminate mainstream financial system
- **ProofOfExistence** with legal importance
- **Blockchain ID**
- **Blockchain changes business**
- **Blockchain changes contract law**
- **Bithalo** as lightweight smart contracting option
- **Ethereum** as a heavy-weight smart cotracting choice
  - Vitali Buterin won a price for that
  - **DAO Ethereum** is revolutionary
  - E.g., **VC raising** with an Ethereum DAO
  - Ethereum is at the forefront of **smart-money** creation
- **Escrows** are the business-model of the future
  - **Smart Contracting HUBs** in Clouds
- **Bitnation 2.0** DIY alternative to stateist government.
DIY Learning

Open-source learning about Blockchains:
- Satoshi Nakamoto's paper about Bitcoins/blockchain
- More papers at the Satoshi Nakamoto Institute
- Many blockchain-tech publications now on scholar.google.com
- Lectures:
  - Harvard free Bitcoin and Cryptocurrency Technology Online Course
  - Princeton Bitcoin and Cryptocurrency lecture
  - Khan Academy has many videos about bitcoins
  - University of Nicosia Master Studies about Bitcoins/Blockchain
- Books:
  - Mastering Bitcoin by Antonopoulos, A.M.
  - Bitcoin and Cryptocurrency Technology, Narayanan, A. et al
  - More on Amazon
Smart Contracts Background

- New enabling concepts and technologies
  - service-oriented cloud computing (SOCC)
  - Business Process as a Service (BPaaS)
  - Cross-organizational eSourcing framework
  - Big data, mobile devices
Sociotechnical Collaboration

Top-down hierarchical organization with disconnected silos

Business-Process Orientation

Lean

How to automate?

CEO + Assistants

Business-Process Management

BPaaS

SaaS

PaaS

IaaS

TaaS

Technical stacks

Business Semantics

Study IT in .ee

sponsored by Skype™

1918
TALLINNA TEHNIKAÜLIKOLL
TALLINN UNIVERSITY OF TECHNOLOGY
Gap Detection

- **Gap:** Existing smart-contract languages do not take into account sociotechnical suitability and expressiveness.
  - Lack of interaction-recognition between acting humans in organizations with technology in workplaces
  - Suitability: concepts/properties to formulate real-world business-collaborations
  - Expressiveness: semantic language-construct clarity for uniform enactment

- **Research question:** How to systematically develop a language and governance platform for cross-sociotechnical and contract-based system collaboration?
  - What is the collaboration context and model the specification language must cater for?
  - What are the main suitability- and expressiveness concepts and -properties?
Business-Collaboration Model
P2P-Collaboration Model
Suitability Exploration

- eContract-based collaboration
  - Who-concept
Suitability Exploration

- eContract-based collaboration
  - Where-concept
Suitability Exploration

- eContract-based collaboration
  - What-concept
Suitability Exploration

**Pattern-based**

- Contractual visibility

---

**DISCOVERING PATTERNS FOR INTER-ORGANIZATIONAL BUSINESS PROCESS COLLABORATION**

ALEX NORTA
Department of Computer Science, University of Helsinki, P.O. Box 68 (Gustaf Hällströminkatu 2b), Helsinki, FI-00014, Finland

PAUL GRENF
Department of Information Systems, Faculty of Technology and Management, Eindhoven University of Technology, P.O. Box 513, NL-5600 MB, Eindhoven, The Netherlands

---

Expressiveness Exploration

- eXchangable Routing Language (XRL)
  - Instance-based workflow language
  - Petri-net semantics and XML syntax
  - Control-flow patterns give strong expressiveness
- Every routing element has WF-net (Petri-net variant) semantics
  - Allows for soundness verification with tool support
- Syntax is a tree
  - Root element with exactly one routing element
  - Simple routing: no children routing elements
  - Complex routing: child-routing elements of specific order
eSourcing Markup Language

- Econtracting Markup Language ECML is foundation
- ECML delta towards eSourcing
  - Incomplete suitability/expressiveness
- Bold eSML definitions are extensions
  - Resource definition
  - Data definition
- Who-extensions
  - resource/data-definition
- What-extensions
  - Control-flow-patterns
- Lifecycle definitions
  - Tasks/processes of collaborating parties
  - Mapped ontologically
Smart-Contract Platform

- Lifecycle of a smart-contract Governance-as-a-Service (GaaS) platform:
  - Startup phase: [paper](#)
  - Rollout & enactment phase: [paper](#)
  - Rollback & termination: [paper](#)

- We use [Colored Petri Nets](#) for designing the GaaS
  - CPN is a graphical oriented language
  - design, specification, simulation and verification of systems
  - CPN-notation comprises
    - states, denoted as circles
    - transitions, denoted as rectangles
    - arcs that connect states and transitions
    - tokens with color, i.e., attributes with values
    - CPN-ML expressions inscripted on arcs
    - modules in CPN are non-atomic place-holder nodes for hierarchic refinements
Startup Phase: top-level lifecycle
Startup Phase: top-level lifecycle
## Setup Collaboration Ontology

<table>
<thead>
<tr>
<th>level</th>
<th>CPN module</th>
<th>data property</th>
<th>description</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>eCommunity lifecycle</td>
<td>sO</td>
<td>service offer that fits a service type</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>sOs</td>
<td>service offer source for communication channel establishment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>sOt</td>
<td>service offer target for communication channel establishment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>pA</td>
<td>partner of an eCommunity</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>rO</td>
<td>role a partner can fill</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>eC</td>
<td>eCommunity identification</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>eCo</td>
<td>eContract based on which partners of an eCommunity transact</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>n,r,k,p,l,q,s</td>
<td>counter variables</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>assigned</td>
<td>service offer assigned to a service type</td>
<td>boolean</td>
</tr>
<tr>
<td></td>
<td></td>
<td>processed</td>
<td>partner prepared for eContract counteroffer re-distribution</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>decision</td>
<td>for negotiated contract proposal (agree</td>
<td>disagree</td>
</tr>
<tr>
<td></td>
<td></td>
<td>outcome</td>
<td>like decision, but input for eCommunity continuation or termination</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>create</td>
<td>bNM</td>
<td>business network model that get populated with service types and roles</td>
<td>integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>m</td>
<td>counter variable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>sT</td>
<td>service type that populates a bNM</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>populate</td>
<td>ch</td>
<td>channel of communication between services</td>
<td>integer</td>
</tr>
<tr>
<td>4</td>
<td>interoperability checking</td>
<td>rOt</td>
<td>role source for communication channel establishment</td>
<td>integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rOs</td>
<td>role target for communication channel establishment</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>contract extraction</td>
<td>spec</td>
<td>specification of extracted eContract</td>
<td>string</td>
</tr>
<tr>
<td>4</td>
<td>agreement finalizing</td>
<td>result</td>
<td>whether all eCommunity partners agree on an eContract proposal or not</td>
<td>boolean</td>
</tr>
<tr>
<td></td>
<td></td>
<td>distributed</td>
<td>contract distributed to partner</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>disagreeing</td>
<td>z</td>
<td>counter variable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>eCo_new</td>
<td>new eContract from a counteroffer to be negotiated</td>
<td></td>
</tr>
</tbody>
</table>
Setup of a Smart Contract

- roles
- number
- NOxNO
- (eC,n)
- m
- 1 (m + 1)
- (eC,sO,pA,rO,true)
- INT
- partners gathered
- NOxNOxNO
- (eC,sO,pA,rO,false)
- if (n > m)
- then 1 (eC,sO,pA,rO, false)
- else empty
- NOxNOxNOxNOxBOOL
- if (n = (m + 1))
- then 1' 1 else empty
- all partners extracted
- NOxNOxNO
- (eC,sO,pA,rO, false)
- if (m > 0)
- and also (r < m)
- then 1' (eC,sO,pA) else empty
- distributed
eContract
proposals
- OUT
- NOxNOxNO
- (eC,sO,sO,sO,t,p)
- NOxNOxNOxNOxNOx Эти слоги
Setup of a Smart Contract
<table>
<thead>
<tr>
<th>level</th>
<th>service</th>
<th>data property</th>
<th>description</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>eCommunity lifecycle</td>
<td>sO</td>
<td>service offer that fits a service type</td>
<td>int</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>sOs</td>
<td>service offer source for communication channel establishment</td>
<td>int</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>sOt</td>
<td>service offer target for communication channel establishment</td>
<td>int</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>pA</td>
<td>partner of an eCommunity</td>
<td>int</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>rO</td>
<td>role a partner can fill</td>
<td>int</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>eC</td>
<td>eCommunity identification</td>
<td>int</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>eCo</td>
<td>eContract based on which partners of an eCommunity transact</td>
<td>int</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>n, r, k, p, l, q, s</td>
<td>counter variables</td>
<td>int</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>assigned</td>
<td>service offer assigned to a service type</td>
<td>bool</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>processed</td>
<td>partner prepared for eContract counteroffer re-distribution</td>
<td>bool</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>decision</td>
<td>for negotiated contract proposal (agree</td>
<td>disagree</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>outcome</td>
<td>like decision, but input for eCommunity continuation or termination</td>
<td>bool</td>
</tr>
<tr>
<td>2</td>
<td>create</td>
<td>bNM</td>
<td>business network model that get populated with service types and roles</td>
<td>int</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>m</td>
<td>counter variable</td>
<td>int</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>sT</td>
<td>service type that populates a bNM</td>
<td>int</td>
</tr>
<tr>
<td>3</td>
<td>populate</td>
<td>ch</td>
<td>channel of communication between services</td>
<td>int</td>
</tr>
<tr>
<td>4</td>
<td>interoperability checking</td>
<td>rOt</td>
<td>role source for communication channel establishment</td>
<td>int</td>
</tr>
<tr>
<td>4</td>
<td>contract extraction</td>
<td>rOs</td>
<td>role target for communication channel establishment</td>
<td>int</td>
</tr>
<tr>
<td>4</td>
<td>agreement finalizing</td>
<td>spec</td>
<td>specification of extracted eContract</td>
<td>int</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>result</td>
<td>whether all eCommunity partners agree on an eContract proposal or not</td>
<td>bool</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>distributed</td>
<td>contract distributed to partner</td>
<td>bool</td>
</tr>
<tr>
<td>4</td>
<td>disagreeing</td>
<td>z</td>
<td>counter variable</td>
<td>int</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>eCo</td>
<td>new eContract from a counteroffer to be negotiated</td>
<td>int</td>
</tr>
<tr>
<td>2</td>
<td>perform</td>
<td>bnma</td>
<td>business network model agent</td>
<td>int</td>
</tr>
<tr>
<td>6</td>
<td>preparation error</td>
<td>l</td>
<td>local service of a respective eCommunity member</td>
<td>int</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>mO</td>
<td>monitor for observing policy adherance of eCommunity partners</td>
<td>int</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>sE</td>
<td>electronic service that is enacted</td>
<td>int</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>lp</td>
<td>local policy extracted from a local contract copy</td>
<td>int</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>lpnr</td>
<td>counter of local policies</td>
<td>int</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>s, x</td>
<td>counter variables</td>
<td>int</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>IC</td>
<td>local contract for respective eCommunity partners extracted from the eContract that coordinates the first</td>
<td>int</td>
</tr>
<tr>
<td>6</td>
<td>contract establishment</td>
<td>insert</td>
<td>service inserting to local contract</td>
<td>int</td>
</tr>
<tr>
<td>6</td>
<td>governance distribution</td>
<td>extracted</td>
<td>instances of contract copies for negotiation</td>
<td>int</td>
</tr>
<tr>
<td>5</td>
<td>prepare</td>
<td>errorID</td>
<td>error identity</td>
<td>int</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>error</td>
<td>error for synchronizing main contract and local copies</td>
<td>int</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>eP</td>
<td>published endpoint for allowing services to communicate</td>
<td>int</td>
</tr>
<tr>
<td>6</td>
<td>preparation error</td>
<td>prepErr</td>
<td>preparation error in the context of assigning an electronic service to a service offer</td>
<td>int</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>assignErr</td>
<td>assignment error in the actual assignment of an electronic service to a service offer</td>
<td>int</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>sEr</td>
<td>service error related to concrete electronic service, e.g., deadlock</td>
<td>int</td>
</tr>
<tr>
<td>4</td>
<td>operate</td>
<td>tc</td>
<td>termination criteria, either full for eCommunity or partial for disruptive partner change that rolls back to a negotiation stage</td>
<td>int</td>
</tr>
</tbody>
</table>
Establishing a decentralized governance infrastructure (DGI)

Rollout Phase

a) Enterprise infrastructure

b) Services
Electronic service choosing & communication-endpoint creation
Disruptively reset
Non-disruptively choose
Non-disruptively choose: remove
Non-disruptively choose: reinsert
Non-disruptively change
Non-disruptively choose: removal
Non-disruptively choose: insertion
Voting options for calming eCommunity conflicts: nondisruptively manage
Voting options for calming eCommunity conflicts: nondisruptively manage
eSourcing Reference Architecture (eSRA)
Mapping the GaaP lifecycle into eSRA

<table>
<thead>
<tr>
<th>DAO-collaboration lifecycle</th>
<th>Service-HUB</th>
<th>eSourcing middleware</th>
<th>Translator</th>
<th>eSourcing setup support</th>
<th>Legacy management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create BNM</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Negotiate eContract</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distribute governance</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare service</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enact eContract</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rollback</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

- Smart contracts miss the application layer on top
  - Primarily technicalities driven bottom-up realization
- eSML for smart contracts evolves out of systematic
  - Top-down sociotechnical suitability/expressiveness exploration
- Real-life contracting foundation for eSML
  - Process-views are subsets of larger in-house processes
- The GaaP in a Cloud serves for managing the smart-contract lifecycle
  - Establishing a decentralized governance infrastructure
  - We choose CPN Tools with formal, graphical modeling semantics
- Stages of the DGI-establishment lifecycle
  - Copy local smart-contract copies per decentralized autonomous organization
  - Extract local policies, monitors, BNMA
  - Configure local services & communication endpoints
- Mapping of lifecycle to eSRA architecture
Thank you for listening!

Q&A

Study IT in .ee

sponsored by Skype™