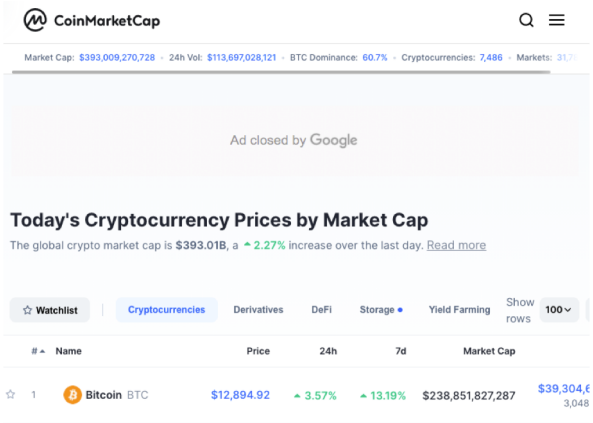
BlockConfess: Towards an Architecture for Blockchain Constraints and Forensics

Sabrina Kirrane & Claudio Di Ciccio

2nd International Workshop on Advances in Artificial Intelligence for Blockchain

@ Blockchain 2020

Blockchain
Information and Communication Technology



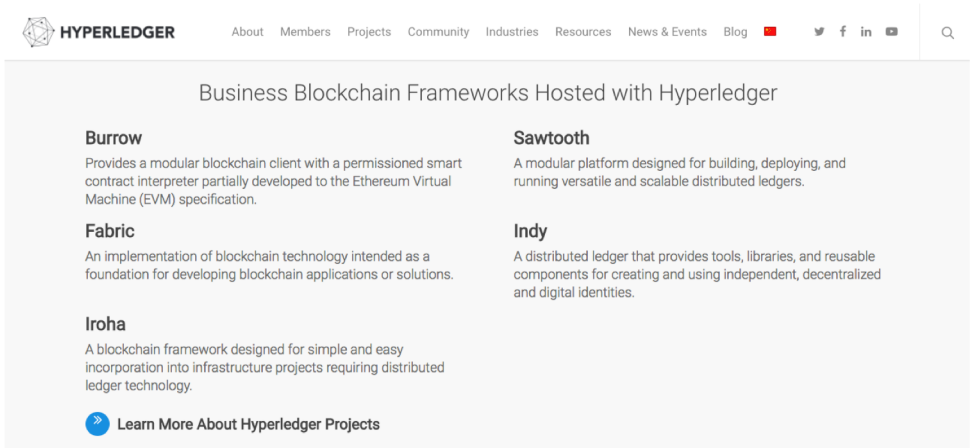
https://coinmarketcap.com/

https://www.cryptocompare.com/coins/guides/how-does-an-ico-work/

https://twitter.com/DigiFinex/s 75
0609880563717

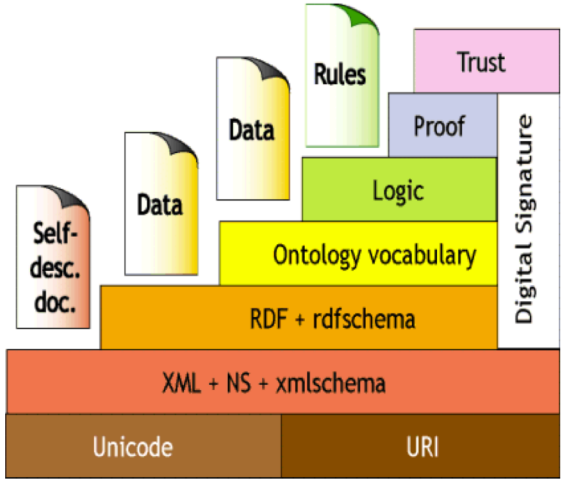
Blockchain
Information and Communication Technology

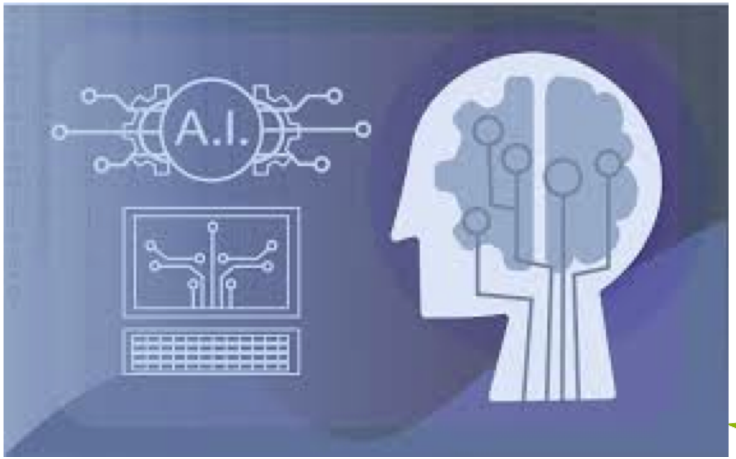
https://www.ethereum.org/

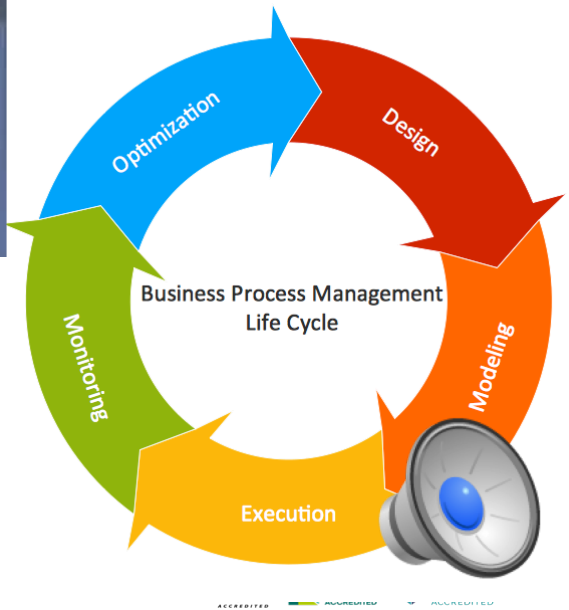


https://www.hyperledger.org/

Information and Communication Technology
Artificial Intelligence



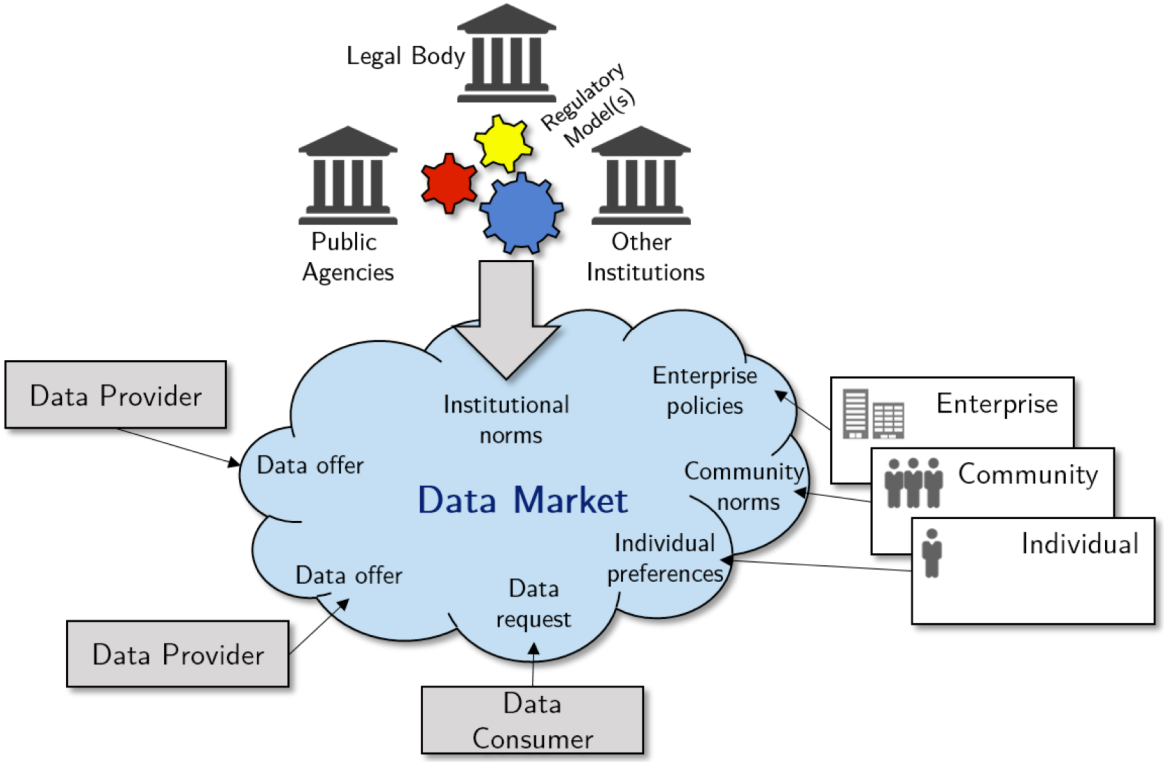




Information and Communication Technology
Executable Code

https://www.pinterest.at/pin/392939136229641306/

Motivating Use Case Scenario
Data Market



If you can't enforce it, contract it: Enforceability in Policy-Driven (Linked) Data Markets, Simon Steyskal and Sabrina Kirrane, International Conference on Semantic Systems (SEMANTiCS), 2015

Motivating Use Case Scenario
Data Market – Executable code - Compliance

- Which **semantic knowledge representation techniques** are needed to describe data and service constraints, as well as relevant metadata and how can we **support automatic enforcement** via the executable code?

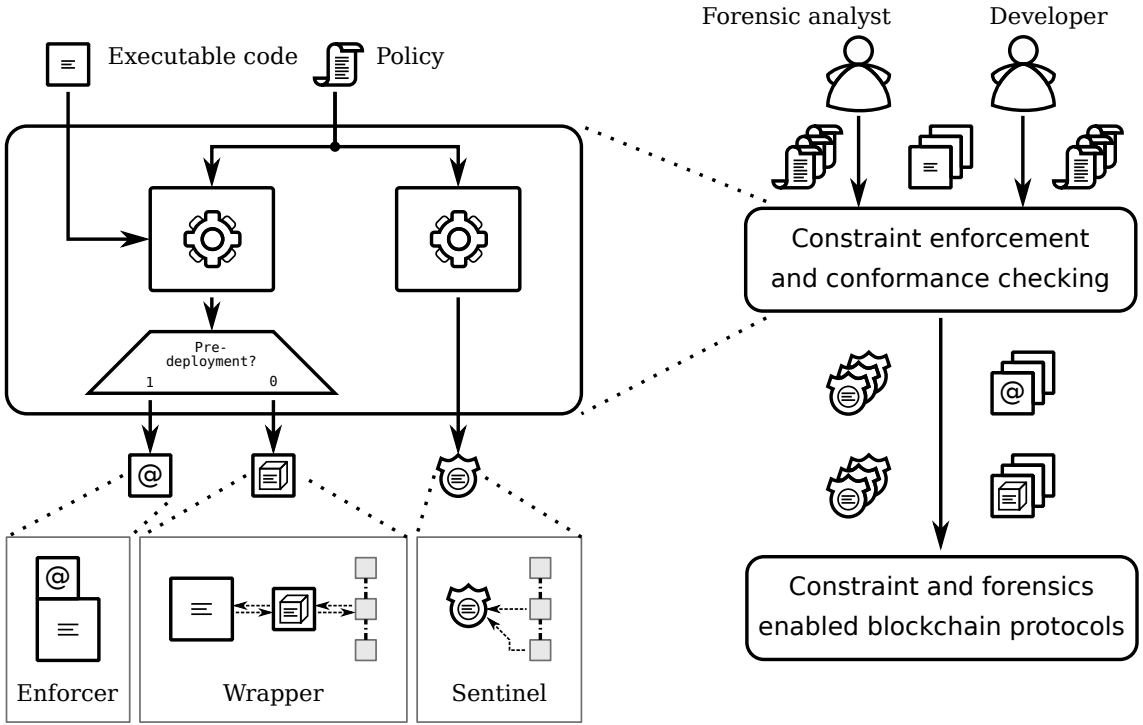
Motivating Use Case Scenario
Data Market – Executable code - Compliance

- How can existing **business process conformance tools and techniques** be modified/adjusted to automatically detect unexpected executable code behaviour (i.e., non conformity, faults, malicious behaviour) in a distributed setting?

Motivating Use Case Scenario
Data Market – Executable code - Compliance

- How do we ensure that both the proposed constraints and forensic tools and techniques are designed in a manner that supports **interoperability and reusability** across various blockchain platforms?

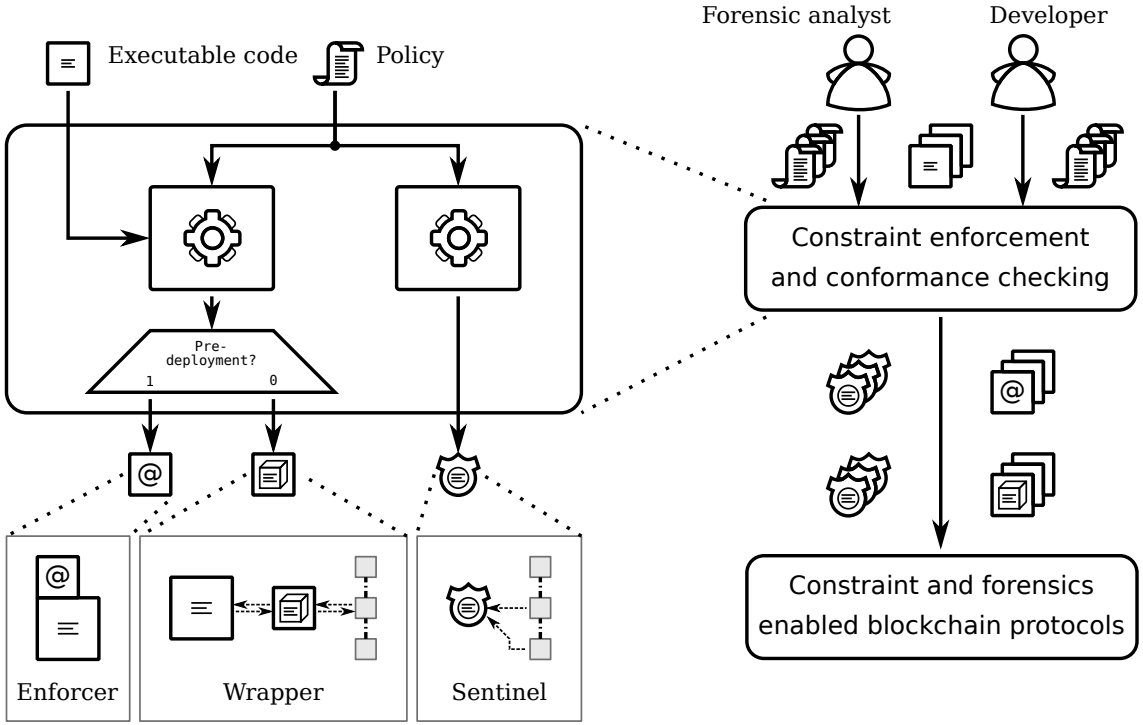
Our Proposal
Conceptual constraint and forensics framework



*Blockchain **executable code constraints**, in the form of usage policies, regulatory obligations, business rules, and societal norms, together with **executable code behavioural forensics** will allow companies to develop innovative services on top of blockchain executable code platforms.*

Conceptual constraint and forensics framework

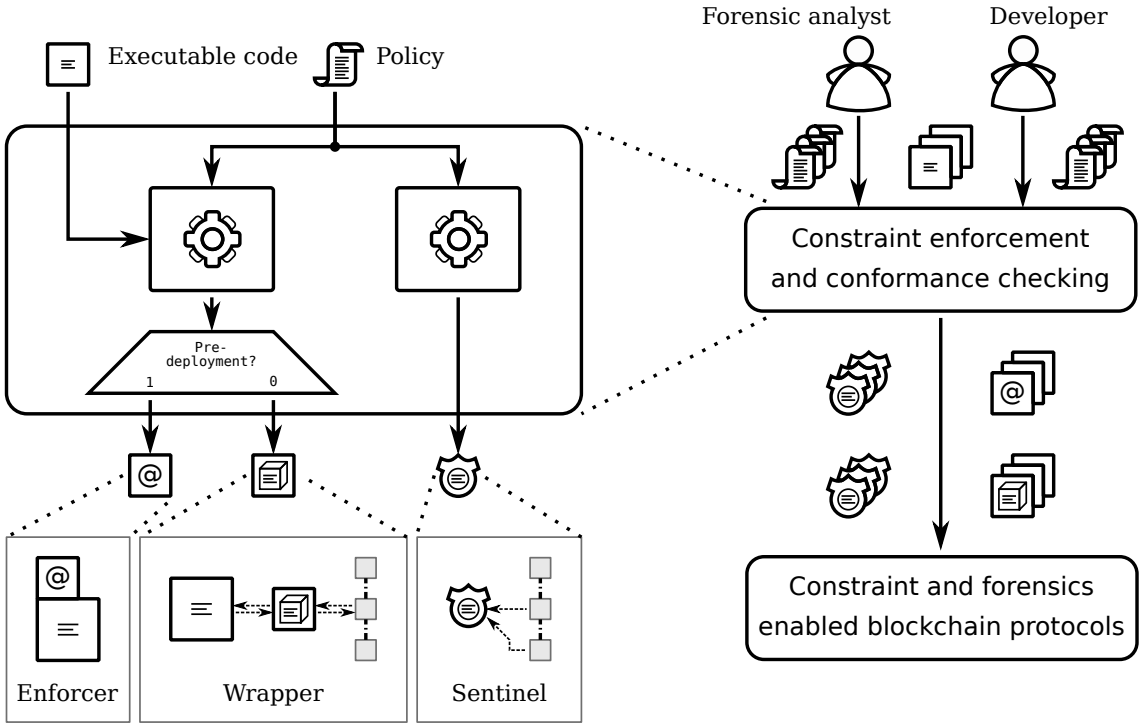
Enforcers



- **Enforcers** are needed to tackle the problem of a-priori constraint enforcement.
- If the **code has not yet been deployed**, the policies need to be turned into encoded statements.
- Assert properties of the code at hand, in a manner that restricts its behaviour thereby **enabling automated compliance checking**.

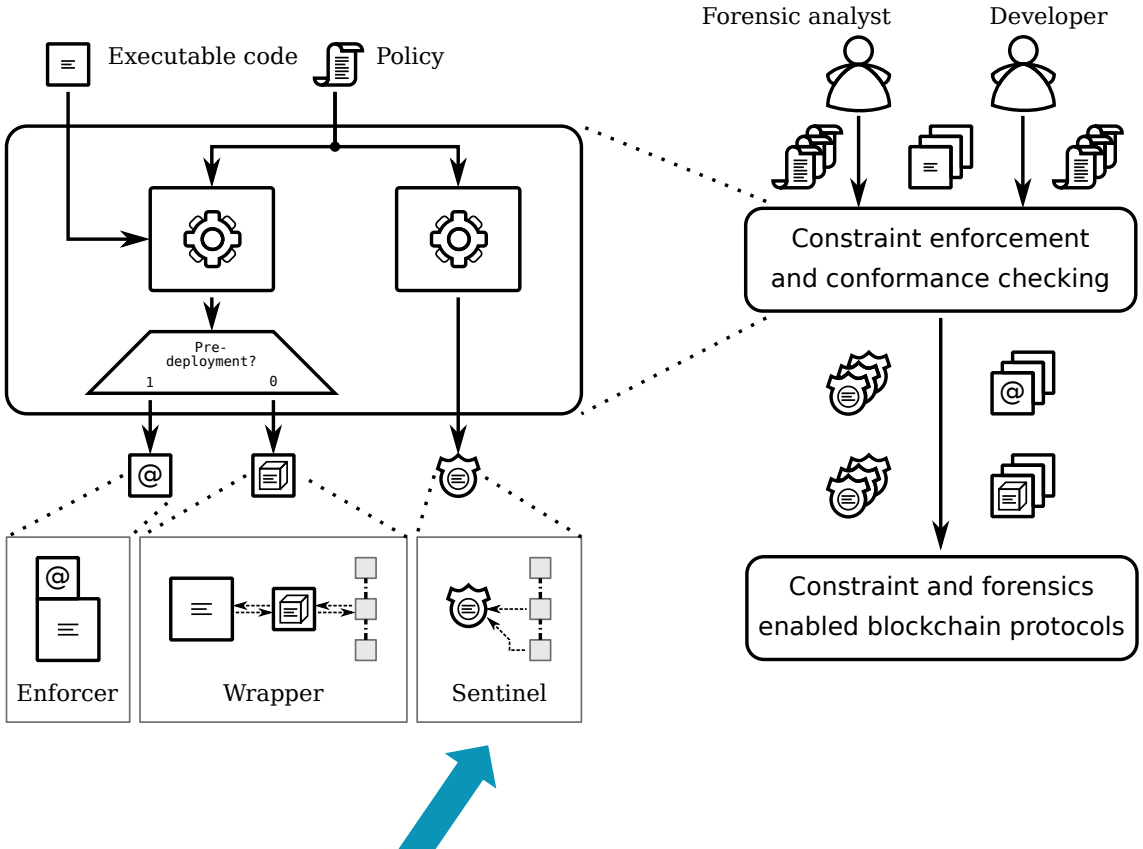
Conceptual constraint and forensics framework

Wrappers



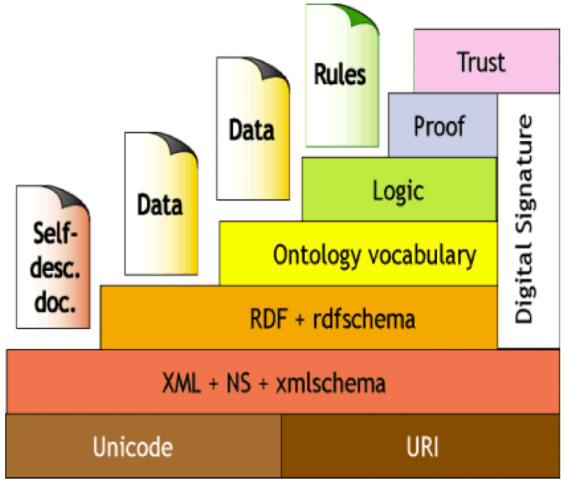
- **Wrappers** also deal with a-priori constraint enforcement, although they are used when executable code is already deployed.
- Wrappers act as a facade, **intercepting and re-routing the messages and transactions.**
- such that deployed applications can also benefit from the **conformance chec**

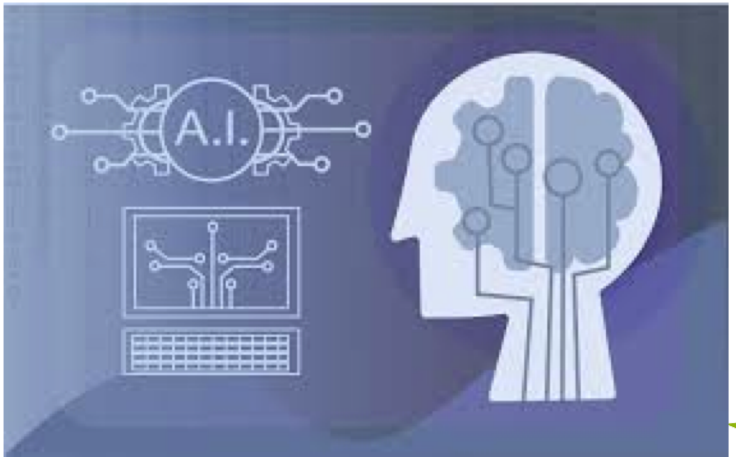
Conceptual constraint and forensics framework
Sentinels

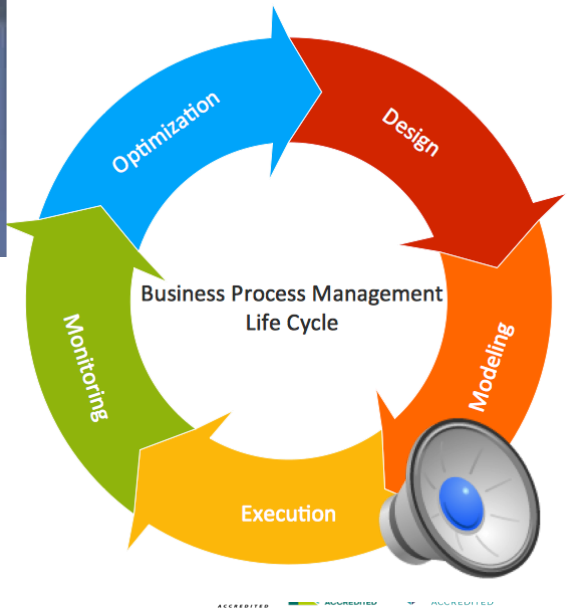


- **Sentinels** focus on the challenge of a-posteriori verification of blockchain executable code based on their recorded transactions.
- Therefore, they query (ex-post) or capture (at runtime) the **transaction flow** into and out of the executable code under analysis.

Information and Communication Technology
Artificial Intelligence







BlockConfess
Constraint specification and enforcement

- From a constraints perspective, there is a need for a **policy language** that can be **adapted/extended** such that it is possible to express a variety of policies.
- Here, general policy languages such as **Rei** and **Protune**, coming from the semantic Web research community, are particularly interesting due to both generality and formal underpinnings.
- The W3C **Open Digital Rights Language** (ODRL) recommendation has been gaining traction in recent years.
- It would be good to leverage the **OWL** based policies provided for by Rei, the **negotiation capabilities** of Protune, and the flexible **profile based extension mechanism** proposed by the ODRL community group.

L. Kagal and T. Berners-lee. Rein : Where policies meet rules in the semantic web. Technical report, Laboratory, Massachusett[illegible] of Technology, 2005.
P. Bonatti, J. De Coi, D. Olmedilla, and L. Sauro. Protune: A rule-based provisional trust negotiation framework. 2010.
M. De Vos, S. Kirrane, J. Padget, and K. Satoh. ODRL policy modelling and compliance checking. In In Rules and Reasoning , 2019.

BlockConfess
Compliance and conformance checking

- From a platform analysis and **business process conformance checking** perspective, it may be possible to adapt existing business process management tools and techniques.
- **Ontology based data access approaches** such as that of Calvanese et al. and **novel object-centric specification languages for processes (e.g., OCBC)** to represent the stateful nature of transactional objects handled by executable code.
- Semantic technologies could be leveraged to **query and reason on the retrieved information** for conformance checking.

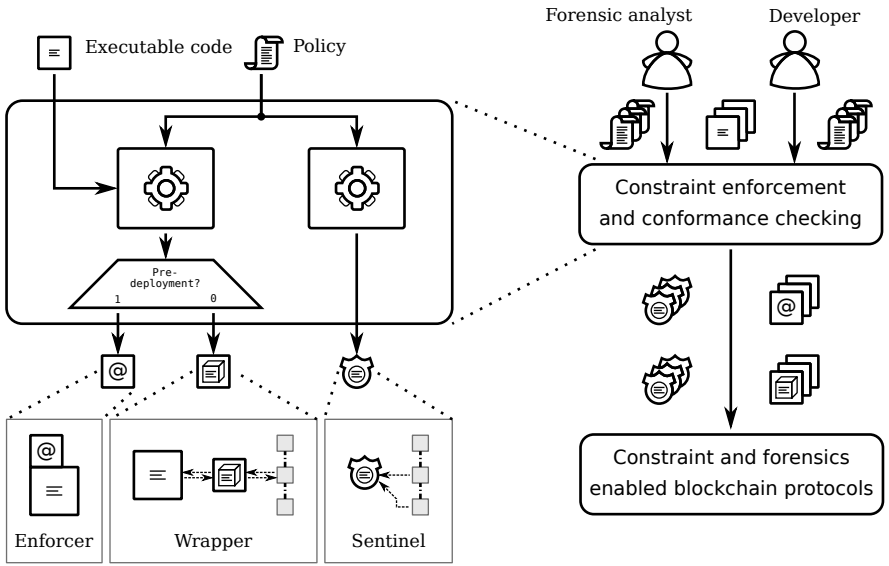
Calvanese, T. E. Kalayci, M. Montali, and S. Tinella. Ontology-based data access for extracting event logs from legacy data: T tool and methodology. In BIS, 2017.
A. Artale, D. Calvanese, M. Montali, and W. M. P. van der Aalst. Enriching data models with behavioral constraints. In Ontology Makes Sense , volume 316 of Frontiers in Artificial Intelligence and Applications, 2019.

BlockConfess
Interoperability and reusability

- When it comes to encoding provenance information related to constraints, processes, logs, etc... the **W3C PROV Ontology** is an obvious choice.
- As for temporal expressions the W3C Spatial Data on the Web Working Group has recently proposed the **OWL-Time Ontology** as a candidate recommendation.
- There are a number of approaches for representing and reasoning over events, such as the **Event Ontology**.
- In order to make executable code interface declarations more accessible, the approach adopted by De Meester et al. could be used to **describe both the function and the metadata** of their implementations.

B. De Meester, T. Seymoens, A. Dimou, and R. Verborgh. Implementation-independent function reuse. Future Generation Computer Systems, 2019.

BlockConfess: Towards an Architecture for Blockchain Constraints and Forensics



- Analyse the **expressivity of existing blockchain executable code** in terms of constraint specification and enforcement.
- Propose **representations** that are suitable for specifying executable code data and service usage constraints paying particular attention to **balancing expressivity and scalability**.
- Adapt/extend existing platform analysis and process **conformance tools and techniques**.
- Develop a **blockchain data marketplace prototype** in order to demonstrate the effectiveness of the proposed techni

Contact Details

VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

Department of Information Systems & Operations
Institute for Information Systems & New Media
Welthandelsplatz 1, 1020 Vienna, Austria

Dr. Sabrina Kirrane

T +43-1-313 36-4494
F +43-1-313 36-90 4494
sabrina.kirrane@wu.ac.at
www.wu.ac.at
www.sabrinakirrane.com
@SabrinaKirrane

This work was partly supported by the Austrian Science Fund (FWF) and netIdee SCIENCE under grant V 759, the COMET cen Austrian Blockchain Center, and the Italian MIUR under grant "Dipartimenti di eccellenza 2018-2022" of the Department of Computer Science at Sapienza University of Rome.