

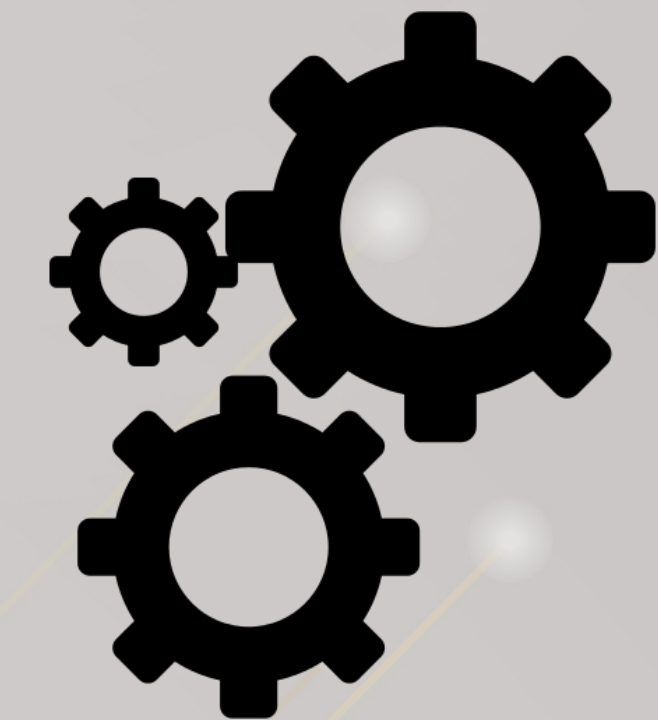
# Reusability of Modeling and Verification Components between the DesignBIP and FSolidM Design Studios

Anastasia Mavridou<sup>1</sup>, Aron Laszka<sup>2</sup>, and Janos Sztipanovits<sup>1</sup>

<sup>1</sup>Vanderbilt University, <sup>2</sup>University of Houston

Design studios facilitate system development by providing system architects with all necessary tools and services for modeling, analyzing, and generating systems.

The modular nature of design studios enables reusability of their components.

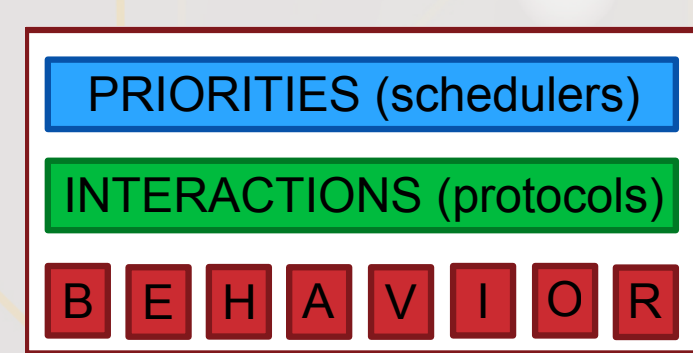
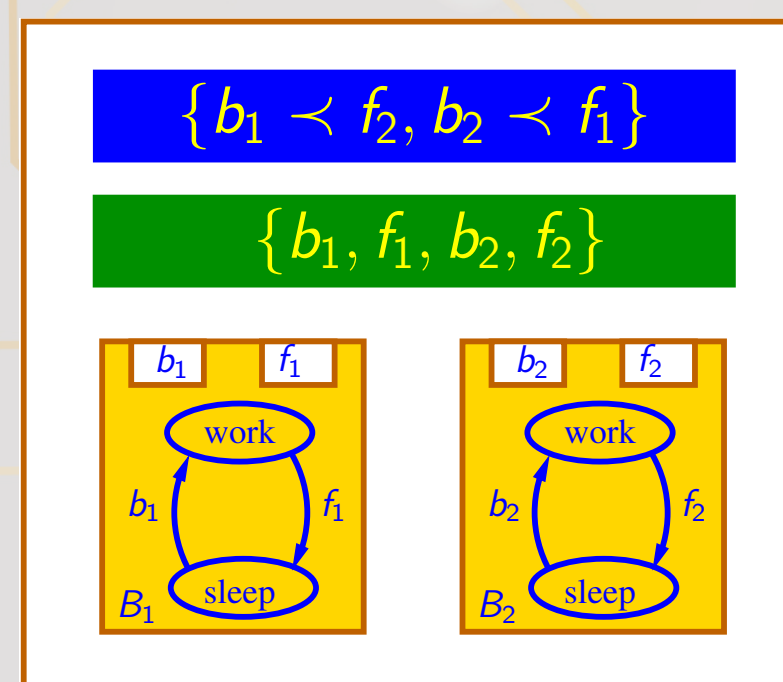


We have developed two design studios: DesignBIP and FSolidM



Promotes rigorous system design:

- Verify first, then generate the code
- A sequence of semantic-preserving transformations
- Provides means for correctness-by-construction
- Parameterized modeling allows coping with model complexity and size
- Integration of NuSMV and simulation/verification tools from the BIP tool-set

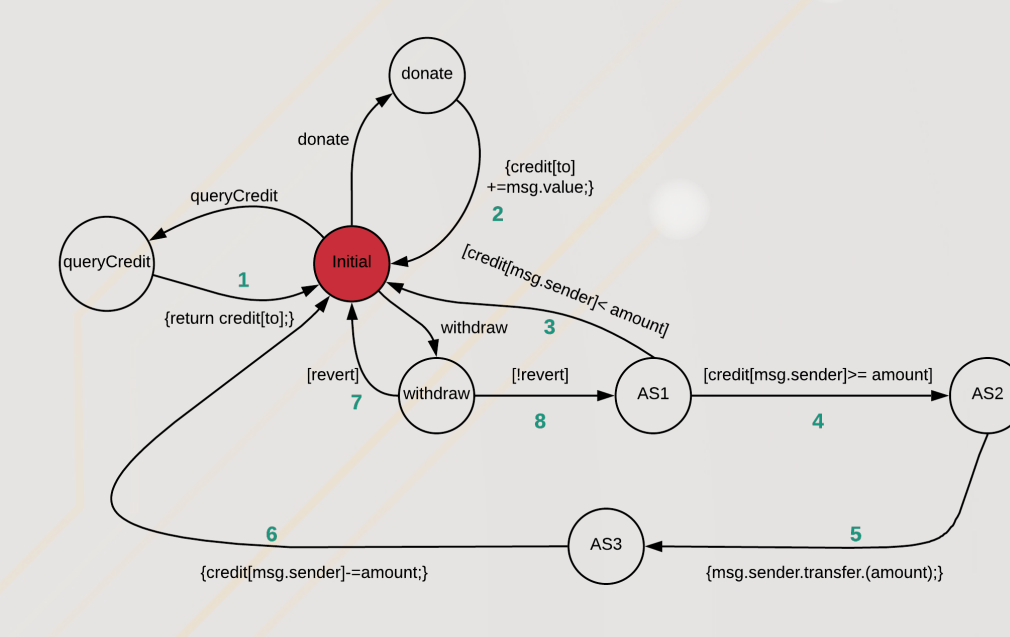


<http://cps-vo.org/group/BIP>



Promotes the development of secure smart contracts:

- Rigorous semantics, FSM-based language
- Equivalent transformation to the BIP language
- Solidity code generation
- Integration of NuSMV and simulation/verification tools from the BIP tool-set
- Integrated, ready-to-use security patterns

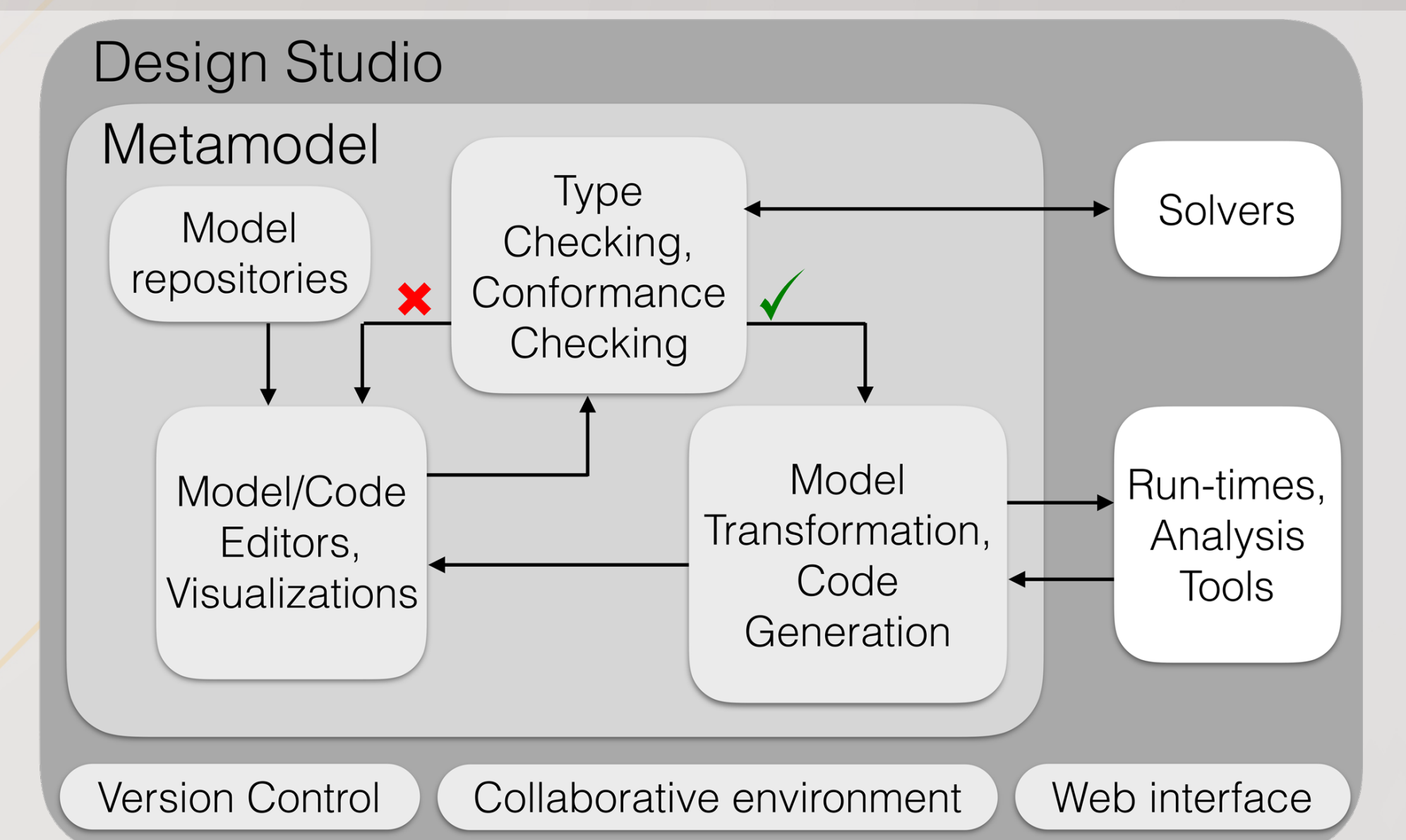


Ethereum

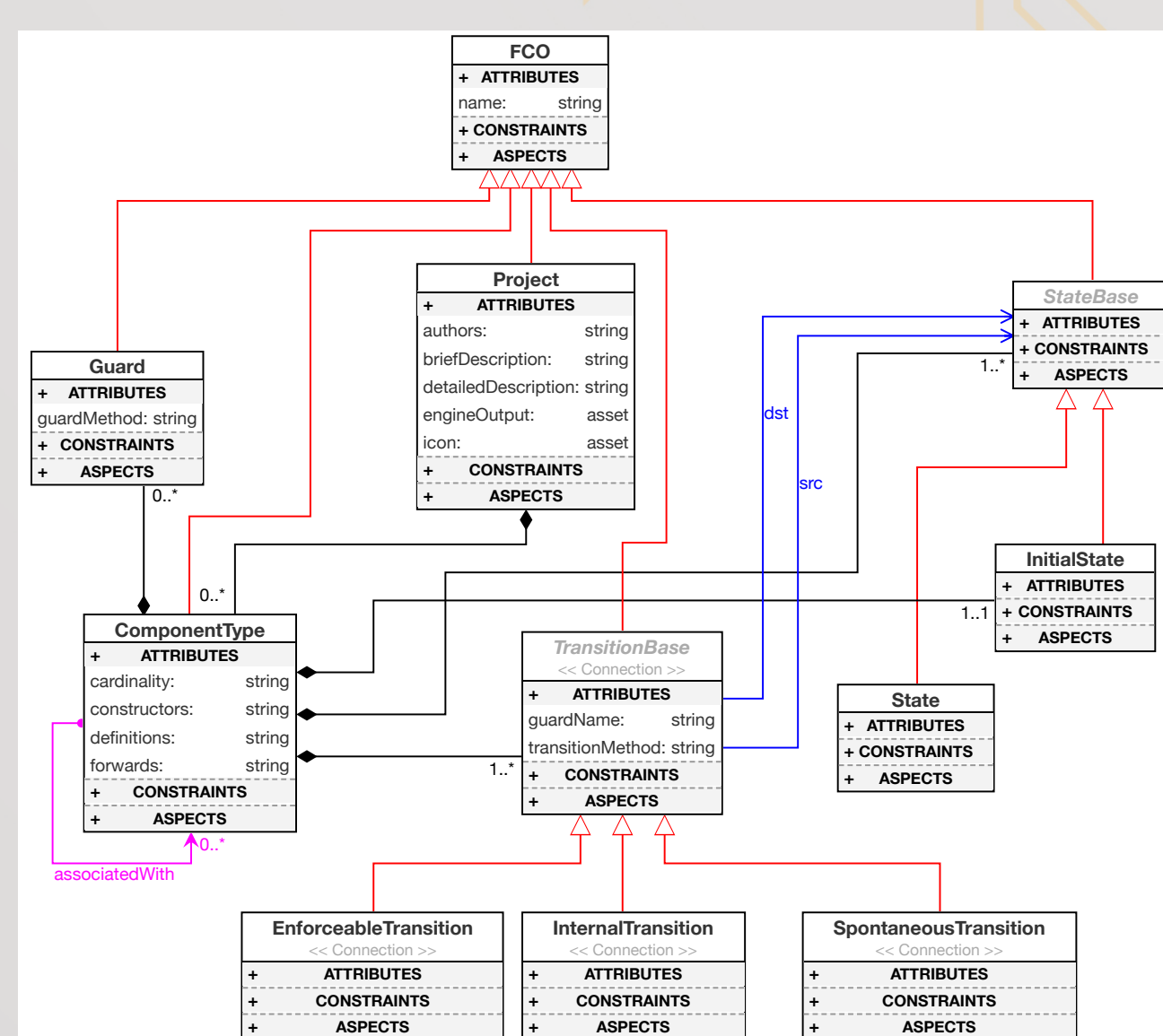
<http://cps-vo.org/group/smartcontracts>

Three main categories of design studio components:

- **Semantic integration components**
  - Domain of the modeling language, i.e., metamodel.
- **Service integration components**
  - Model editors, code editors, model transformation, code generation, consistency checking, model repositories, version control, etc.
- **Tool integration components**
  - Simulation, verification tools, etc.



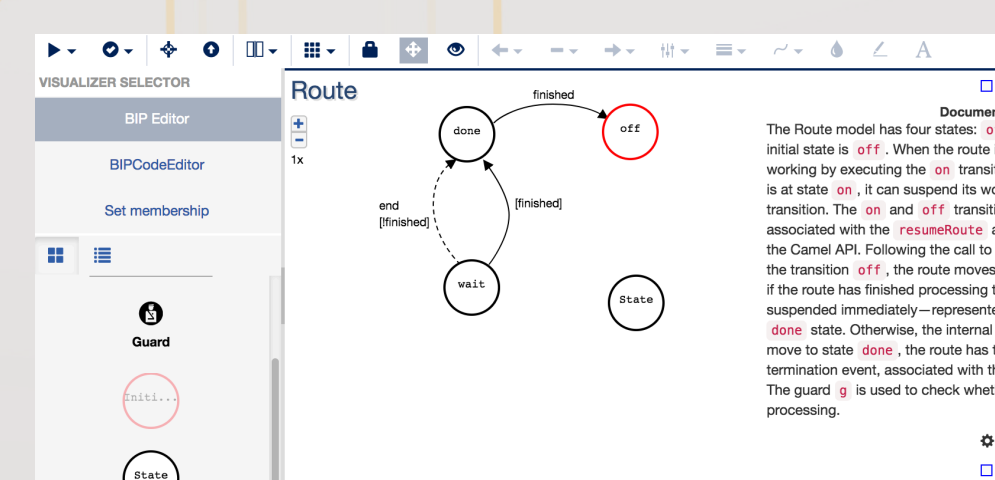
Reusability of semantic integration components



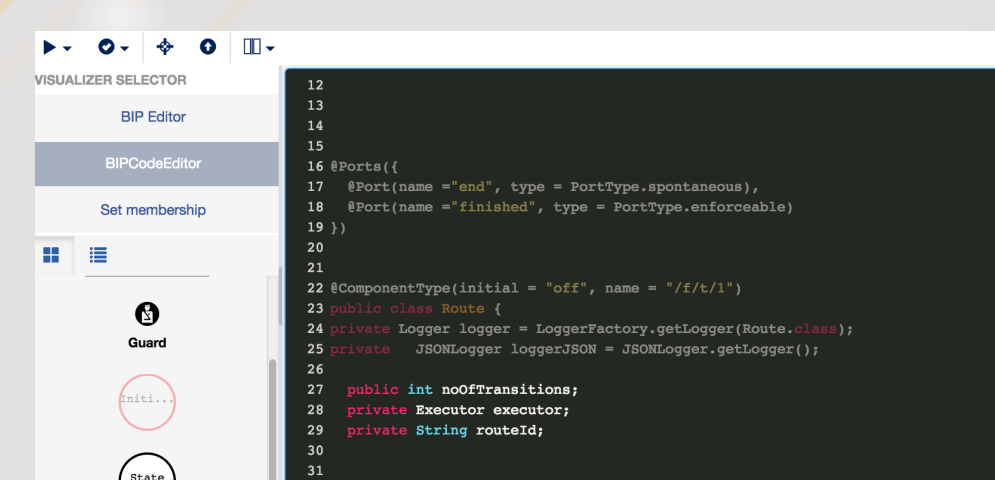
BIP language

Reusability of service integration components

1) FSM-model editor:



2) Code editor:

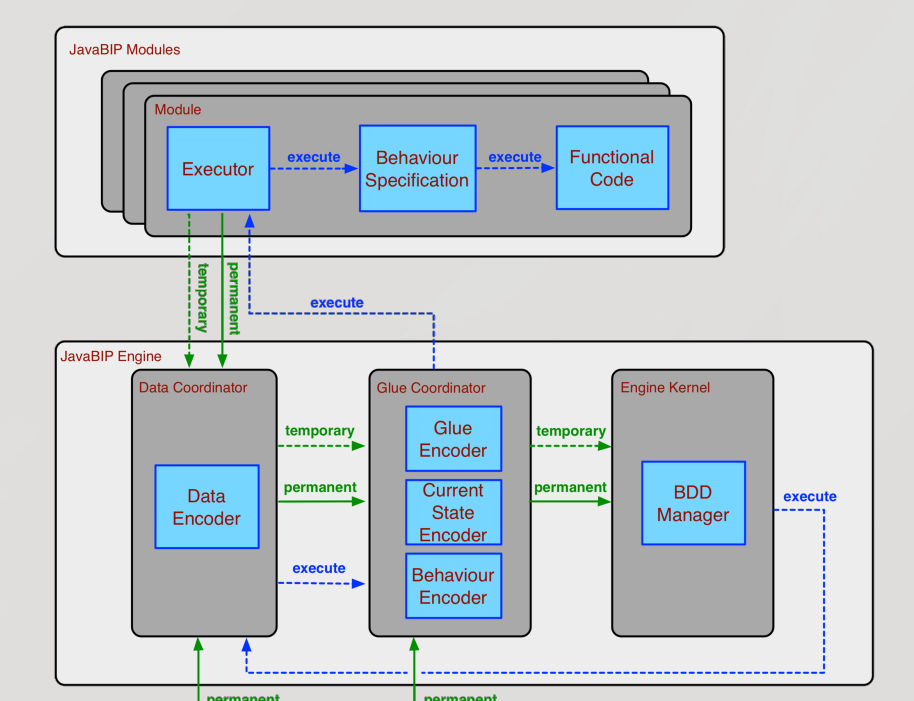


3) BIP-to-NuSMV transformation

Reusability of tool integration components



NuSMV model checker



BIP-engine



Microsoft's FORMULA

## References

- [1] Anastasia Mavridou, Joseph Sifakis, and Janos Sztipanovits. "DesignBIP: A Design Studio for Modeling and Generating Systems with BIP." MeTRiD. 2018.
- [2] Anastasia Mavridou and Aron Laszka. "Tool demonstration: FSolidM for designing secure Ethereum smart contracts." POST. 2018.
- [3] Anastasia Mavridou and Aron Laszka. "Designing Secure Ethereum Smart Contracts: A Finite State Machine Based Approach." FC. 2018.



THE EIGHTEENTH ANNUAL  
HIGH CONFIDENCE  
SOFTWARE AND SYSTEMS  
CONFERENCE

Annapolis, MD | May 7-9, 2018