



Blockbird Ventures

# BlockSim – Blockchain Simulator

Miguel P. Correia

Joint work with Carlos Faria

74<sup>th</sup> IFIP WG 10.4 Meeting, Clerveaux; Luxembourg Jun.-Jul. 2018

**U LISBOA** | UNIVERSIDADE  
DE LISBOA



**FCT** Fundação para a Ciência e a Tecnologia  
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR



# Blockchain introduction



# Our work

- There is a lack of **tools to test blockchains** and answer questions like:
  - What's the impact of changing certain parameters?
  - How will my company's blockchain perform?
- **Running** the blockchain is often not practical
  - 1000s nodes in a WAN, time, energy consumption,...
- Our work: **BlockSim blockchain simulator**
  - 1<sup>st</sup> phase: permissionless blockchains (PoW-based)
  - 2<sup>nd</sup> phase: permissioned blockchains (BFTconsensus-based)

# What is simulation?

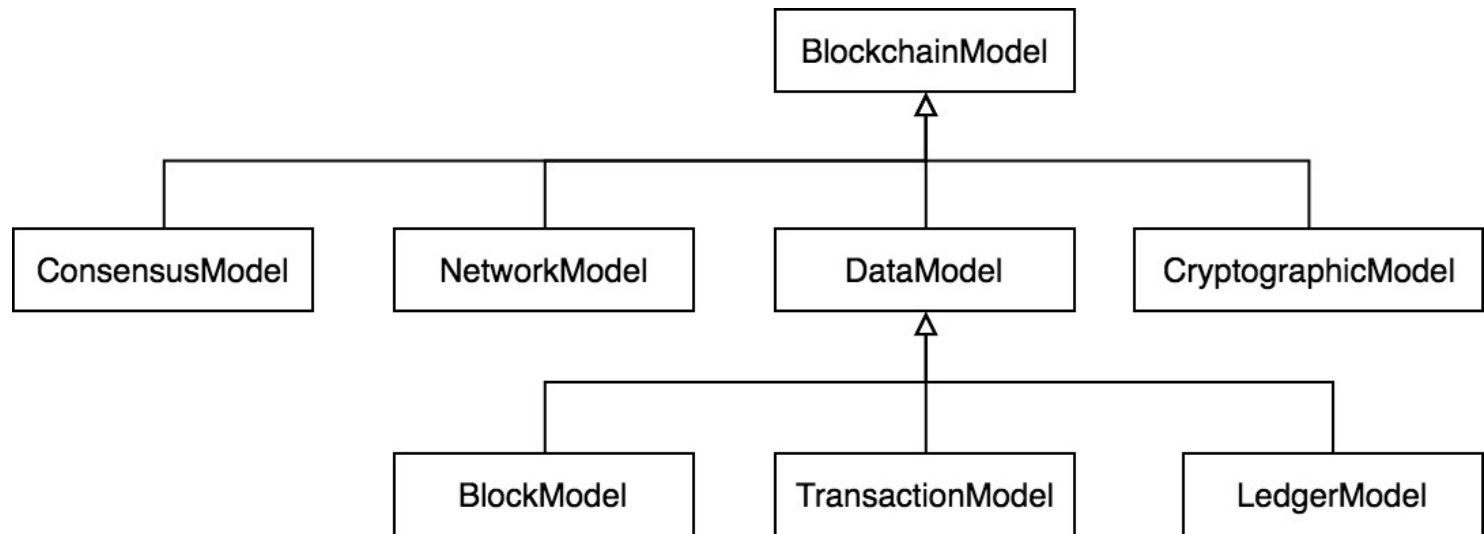
- Reproduction of the operation of a system over time; a simulation “runs” a **model** instead of the system
- **Simulators** can be classified as:
  - **stochastic or deterministic** – model events probabilistically or not
  - **dynamic or static** – system can change or not
  - **discrete-event or continuous** – work on a sequence of events or a continuous process

# BlockSim

- A **flexible** blockchain simulator to evaluate **several blockchains** on large scale networks
  - Based on **abstract models**, which can be instantiated to different blockchains (permissionless and permissioned)
- Simulation models:
  - **Stochastic**: probabilistic phenomena
  - **Dynamic**: system changes over time
  - **Discrete-event**: only keep track of system state changes

# BlockSim Modeling Framework

- Set of abstract classes that are extended with variables and methods for specific blockchains
- BlockSim provides the former classes and runs the latter



# Example Bitcoin simulation steps

1. **Identify the question** to be answered  
*e.g., what is transaction rate with 4MB block size?*
2. **Define the models:** transaction, network, consensus...
3. Define the **parameters** for each model  
*e.g., block interval distribution and miners' mining hash power*
4. **Collect measurements** from the Bitcoin network and instantiate probabilistic models
5. **Code the models** following the modeling framework
6. **Simulate** and obtain results

# BlockSim Status

- **Simulator and modeling framework** for permissionless blockchains (1<sup>st</sup> phase) implemented
  - 2<sup>nd</sup> phase about to start
- **Instantiations** for Bitcoin + Ethereum almost done
- **Validation** about to start
- There are a few **other simulators**
  - Not stochastic
  - Not flexible (e.g., focused on Bitcoin)
  - Don't model e.g. the CPU (e.g., delay due to crypto)





Blockbird Ventures

# Thank you

Miguel P. Correia

<http://www.gsd.inesc-id.pt/~mpc/>

<https://blockbird.ventures/>