Modeling and Simulating Blockchain Systems

Paris Blockchain Week Summit

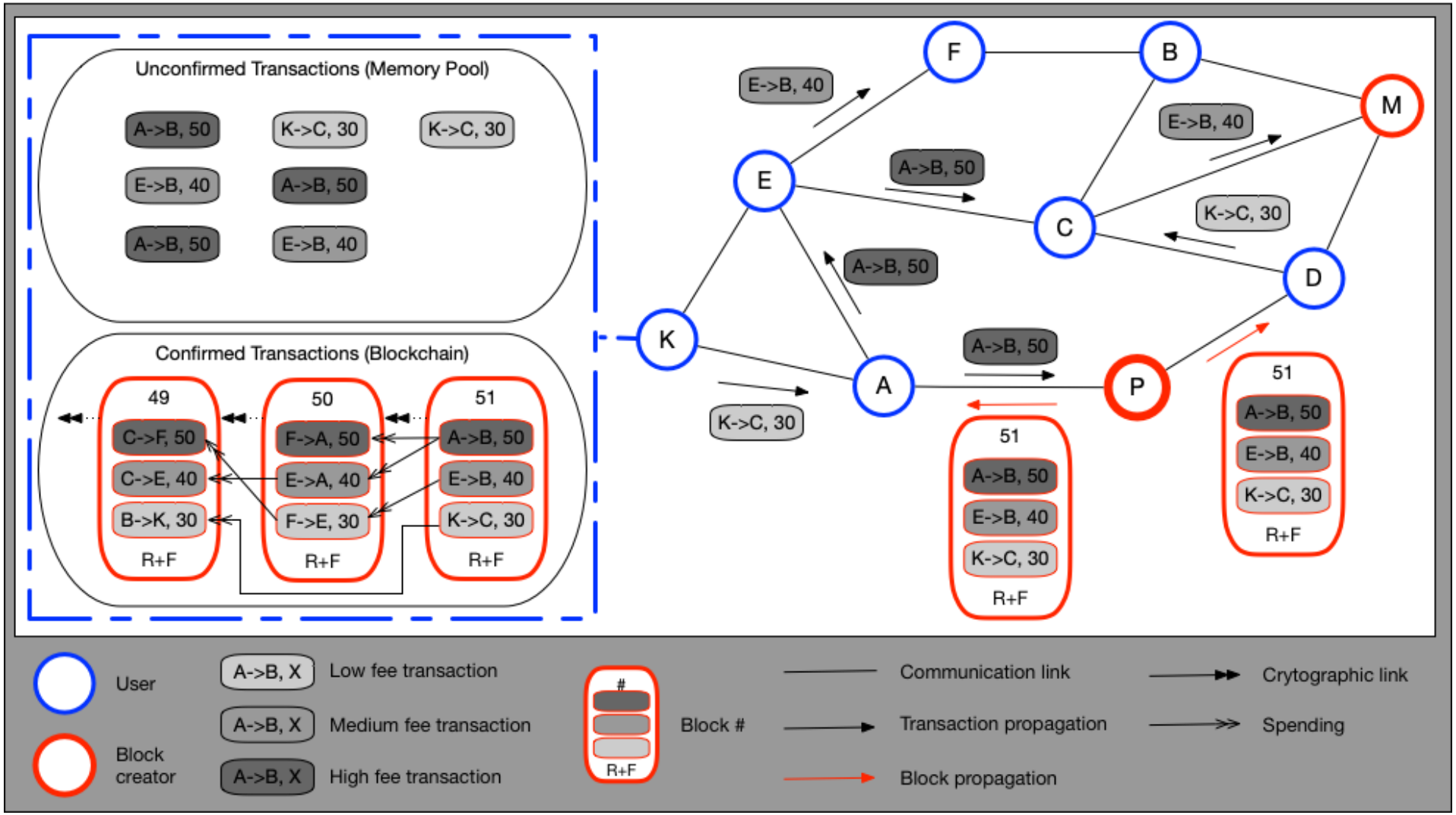
Önder GÜRCAN, PhD., Research Engineer, Expert

9 December 2020

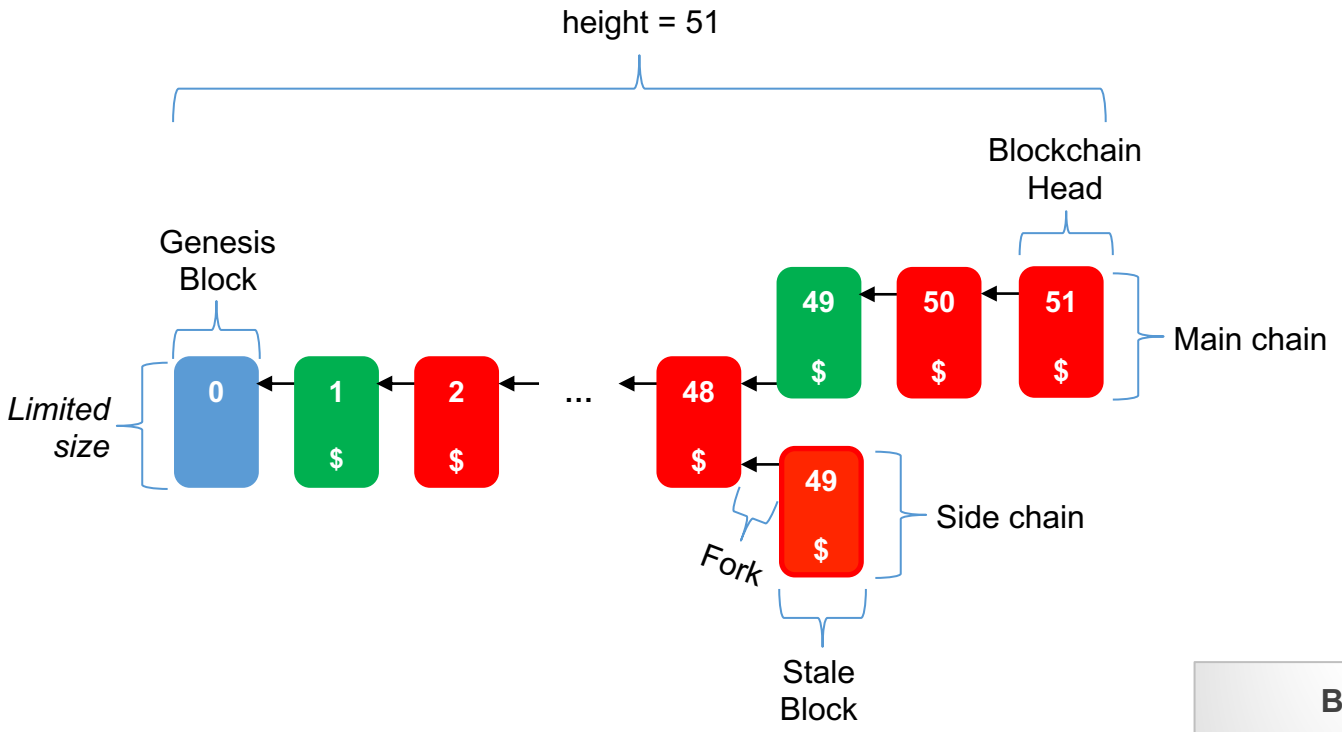
The Blockchain

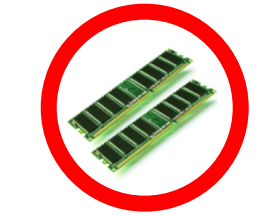
- The blockchain is a registry that contains the history of all exchanges made between its users since its creation.
- The exchanges are stored in the blockchain in a secure, tamper-proof and transparent way.

Blockchain System

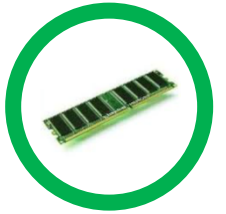


Anatomy of a Blockchain



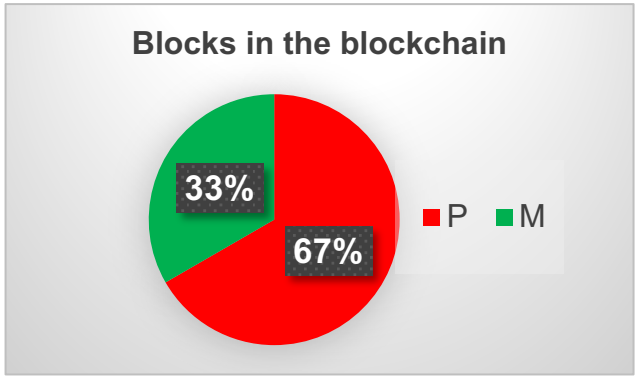


Block Creator P



Block Creator M

Quality of the chain



Blockchain Systems

- Blockchain systems are distributed systems
  - A distributed system is a collection of independent computers that appears to its users as a single coherent system [Tanenbaum et al. 2007].
  - A distributed system is one in which the failure of a computer you did not even know existed can render your own computer unusable [Lamport 1987].

Blockchain Systems (cont.)

- Blockchain systems are social organizations
  - Social organizations are formal or informal groups of interrelated individuals (agents) who pursue a collective goal and who are embedded into an environment [Ostrom 2009].
  - The blockchain (data structure) is a physical manifestation of the interactions of users.
  - Blockchain systems facilitates cooperation by getting self-interested, distrustful actors to work together.
  - Conflict of individual/collective goals (e.g., users want lower fees while block creators want higher fees) [Gürcan et al. 2017].
  - Continuous enter/exit dynamics [Gürcan et al. 2017].

Blockchain Systems (cont.)

- Blockchain systems are economical systems
  - S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
  - An economical system, as any other complex system, reflects a dynamic interaction of a large number of different agents, not just a few key agents.
  - The resulting systemic behavior, observable on the aggregate level,
    - often shows consequences that are hard to predict
      - e.g., the transaction fees
    - which cannot be simply explained by the behaviors of a few major agents.

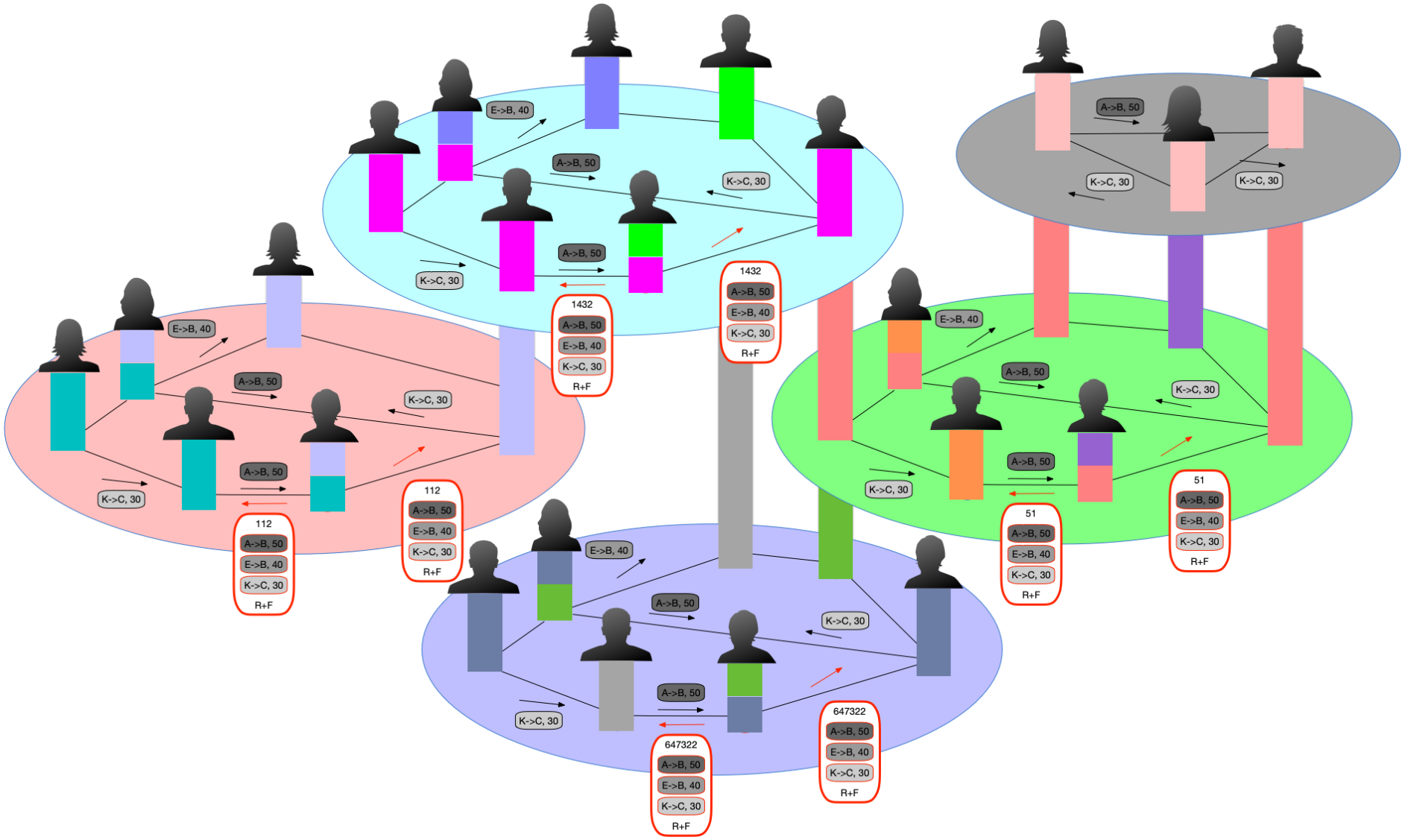
Moreover…

- We face highly competitive (and complex) industrial cases
  - that have technical problems: data reliability, confidentiality, identification, archiving, ….
  - which are being constantly reshaped by client demands, technology and regulatory requirements.
    - Client demands: e.g., performance (# of transactions/minute), fees …
    - Technology: e.g., (blockchain) protocol, parameters, cost …
    - Regulations: e.g., standards, laws, GDPR …
- Blockchain ecosystem is very active and dynamic.
  - Bitcoin, Ethereum, Tendermint, Hyperledger, Sycomore, etc.

Challenge

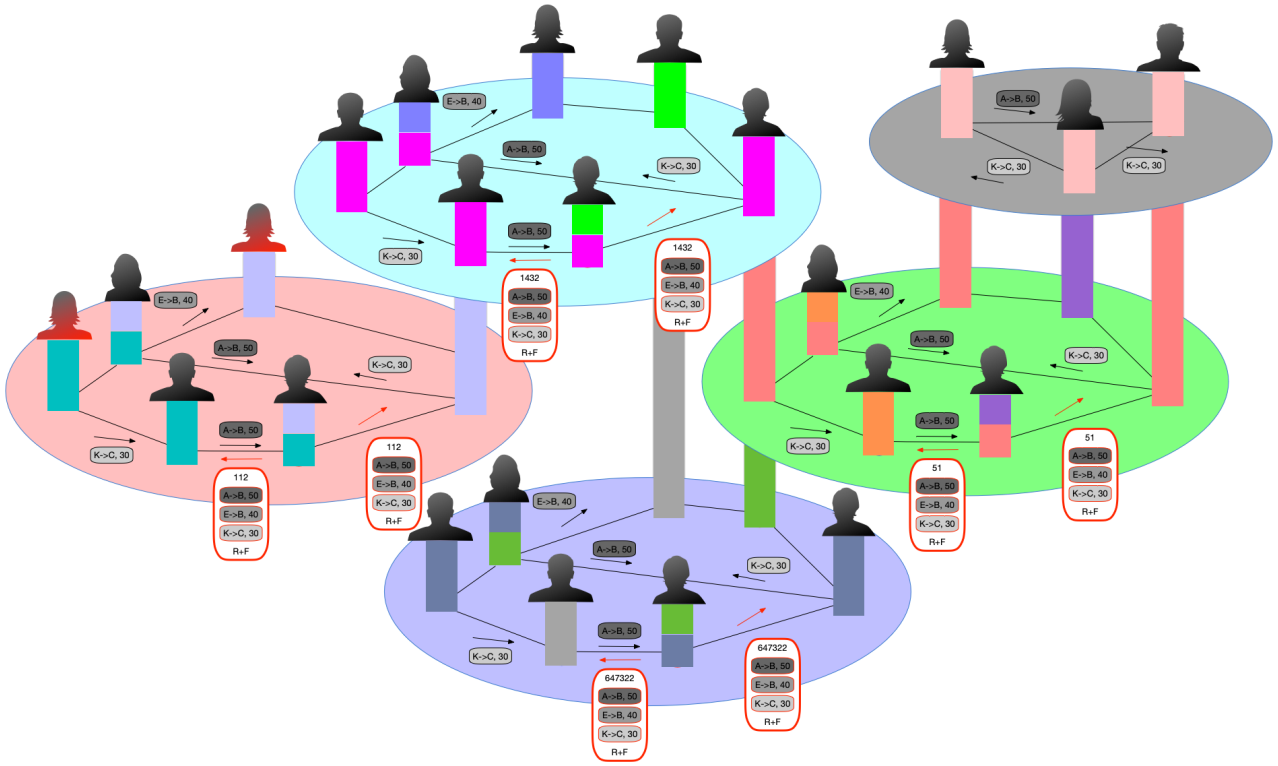
- Carrying out feasibility analysis in a realistic manner,
- Rapid prototyping of new solutions,
- Benchmarking of existing/new solutions,
- Thus, we need
  - a well-defined modeling approach provides necessary abstractions,
  - a next-generation simulation framework, which is develop as a software using modern engineering approaches
    - (e.g., modularity - i.e. model reuse-, testing, continuous development and continuous integration, automated management of builds, dependencies and documentation)
  - and agile principles

Modeling Blockchain Systems [Gürcan 2019]

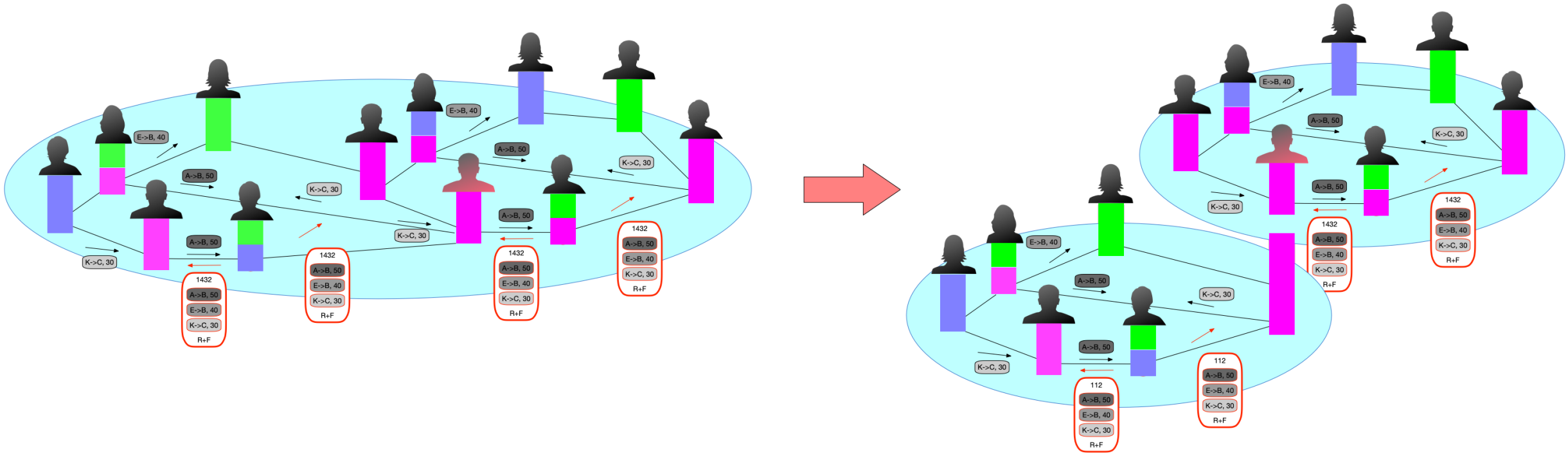


Studying Fairness in Blockchain Systems

- **What is fairness?**
  - Satisfaction of the participants from the system [Gürcan et al. 2017].
- **Why is fairness important?**
  - **Satisfied participants** -> tend to **stay** in the system
  - **Unsatisfied participants** -> tend to **leave** the system
  - # of participants ↗️ -> security and stability ↗️

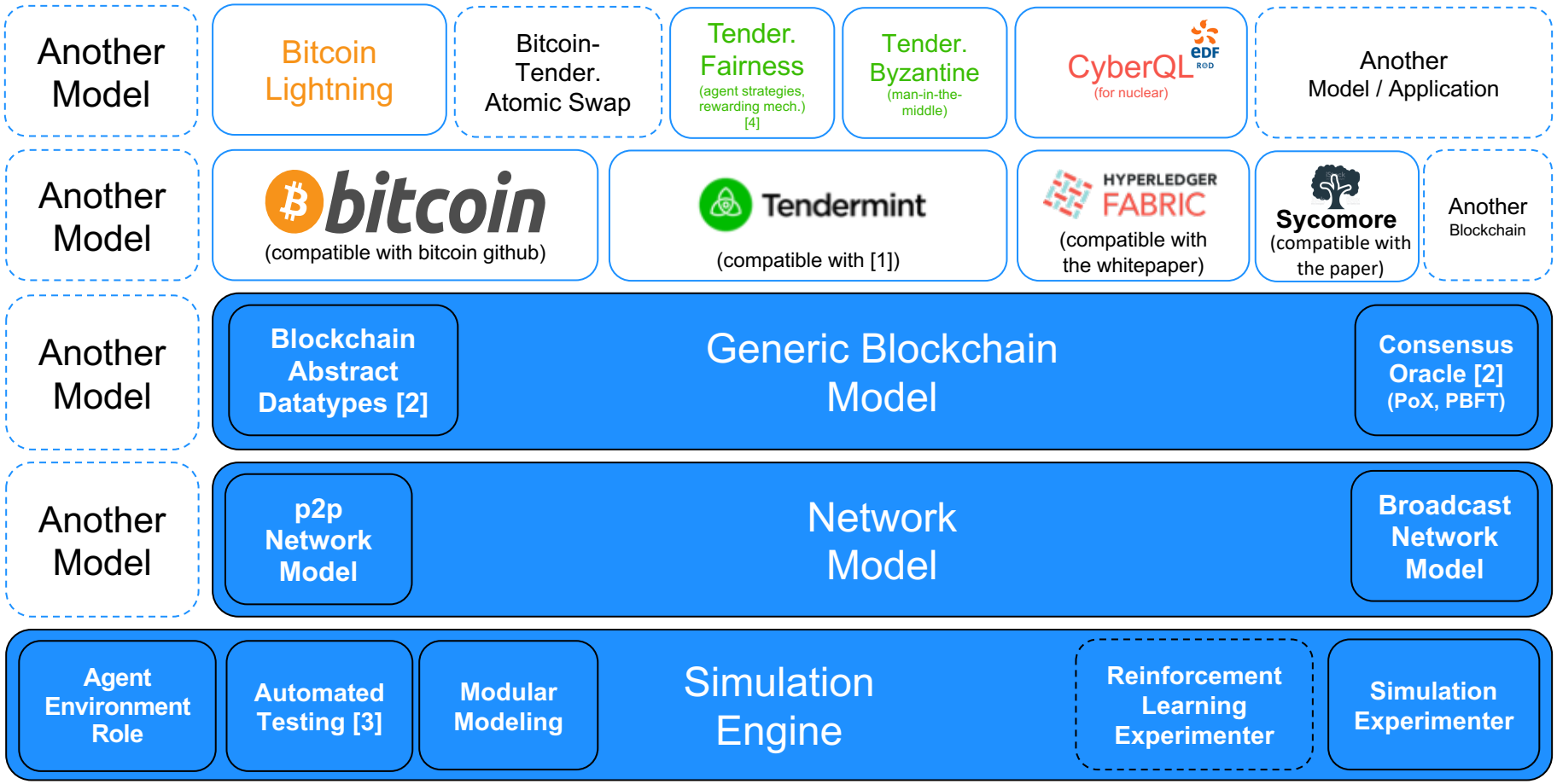


Studying Attacks in Blockchain Systems



e.g., Man-in-the-middle attack

Multi-Agent eXperimenter



ADACORSA

REACH

[1] Y. Amoussou-Guenou, A. Del Pozzo, M. Potop-Butucaru, and S. Tucci-Piergiovanni, **Dissecting Tendermint**, International Conference on Networked Systems (NETYS 2019), pp 166-182, 2019.
[2] E. Anceaume, A. Del Pozzo, R. Ludinard, M. Potop-Butucaru, and S. Tucci-Piergiovanni, **Blockchain Abstract Data Type**, in SPAA 2019, Phoenix, AZ, USA, June 22-24, 2019., 2019, pp. 349–358.
[3] Ö. Gürcan, O. Dikenelli, C. Bernon (2013). **A generic testing framework for agent-based simulation models**. Journal of Simulation.
[4] N. Lagaillardie, M. A. Djari, Ö. Gürcan (2019). **A Computational Study on Fairness of the Tendermint Blockchain Protocol**. Information.

Conclusions

- Blockchain systems domain is multi-disciplinary:
  - Distributed systems, social organization theory, economy, software engineering etc.
- For **realistic modeling and simulation** of blockchain systems, we need an **analytical tool** that provides necessary **abstractions** and properties
  - **agent-based modeling,**
  - **Agent/Environment/Role** organization model,
  - reusable models (integrated via modern build management tools),
  - automated **testing** (integrated to standard testing tools like JUnit)
    - allows CI/CD: automated management of builds, dependencies

Thank you for your attention!

Önder GÜRCAN