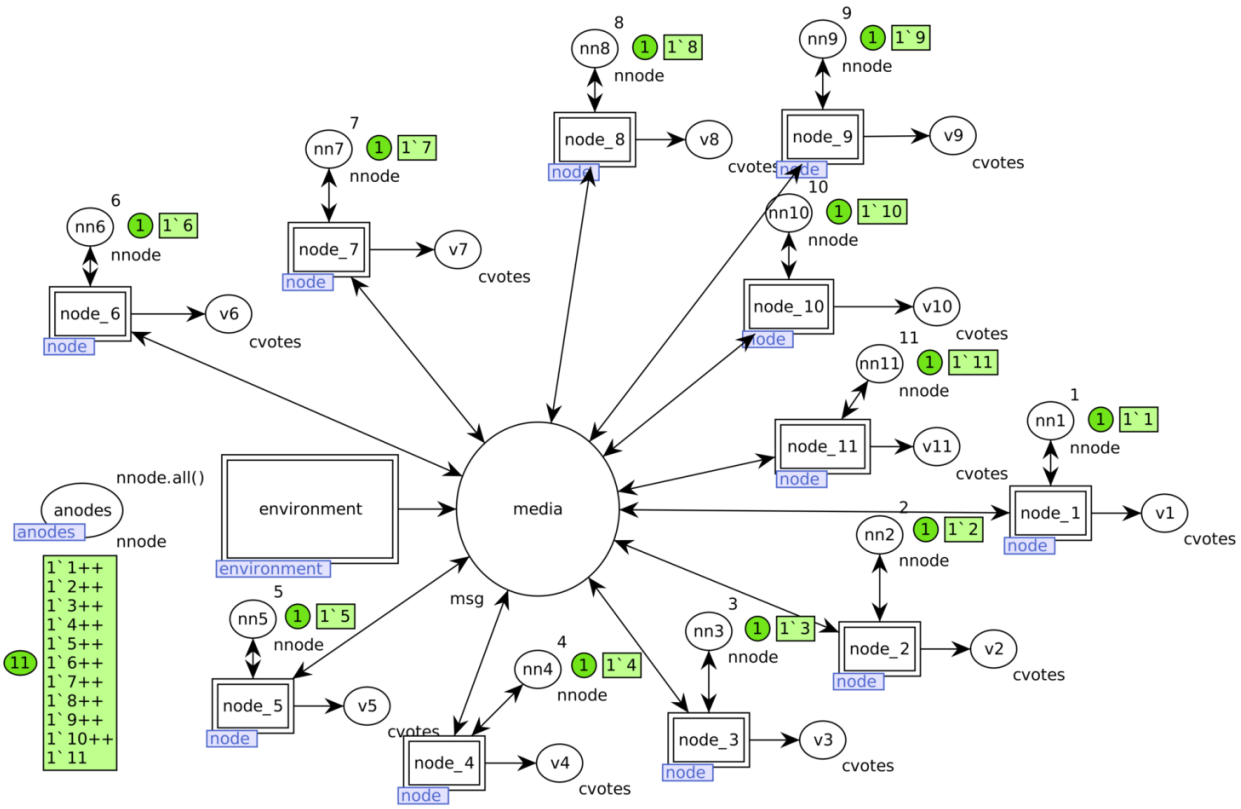
Proof-of-work agreement protocol

The model implements an agreement (consensus) protocol for proof-of-work blockchain cryptocurrency similar to Bitcoin. It takes into consideration possible attacks on network, represented as growing the maximal message delivery time, and Byzantine fault tolerance inserting certain part of Byzantine nodes with an arbitrary answer. Nodes of the network are represented in explicit graphical form. Among the model parameters are: the range of voted values; the threshold for approving votes; parameter of exponential distribution of time between node activation messages; the maximal message delivery time.



This model is described in:

Birgit Pröll, Werner Retschitzegger, Wieland Schwinger, Tatiana R. Shmeleva & Dmitry A. Zaitsev, Modelling proof-of-work agreement protocol by coloured Petri nets, International Journal of Parallel, Emergent and Distributed Systems, 37(6), 2022, 597-612.

Proof-of-work agreement protocol, offered by Keller and Böhme, is analysed by coloured Petri nets and refined. Blockchain technology, based on proof-of-work procedure and Nakomoto consensus negotiations, represents fundamentals of many kinds of cryptocurrency widespread recently. The protocol, called A_k, works in continuous time which is simulated using random exponential distribution function of CPN Tools system, obtained values rounded to map them into discrete time of a coloured Petri net. Hierarchical model consists of an environment subnet and a given number of nodes communicating via an unstructured network represented by a single place; the

model of node is further structured based on event handlers of the protocol source specification such as initialisation, activation, message delivering, and termination condition check. Based on the simulation results, modifications of the protocol and its parameters are recommended which improve some imperfections of the protocol.