Multi-Agent Systems
Understanding blockchain communication using epistemic logic

June 27, 2021

Blockchain and epistemic logic

The blockchain logic we propose is based on [1] and uses the concepts of T-consistency, which is related to the content of the ledger and weak growth, which is related to the length of the ledger. These are further explained in the following subsections.

We will be using the following definitions throughout our logical arguments:-

- `Agent's history:` It is includes the agent's initial state and its sent/received transactions until a given time.
- `Environment state:` It keeps track of important features such as, list of all agents at time t, identity of honest agents at a given time, etc.
- `Global state:` It includes the local state of all agents plus the environment state.
  (Note: Since the global state is dynamic in a blockchain and changes with time. Hence a temporal component is needed in the model, which will change the definition of the global state, as described in the later subsections.)
- `Run:` It is a function mapping a given timestamp to a global state.
  Following shows different runs of the protocol at time 0 and 1:-
  1. Initial global state = r(0)
  2. Next global state = r(1)

  (Note: the time is taken to be a natural number here, hence we are starting with 0.)
- `System:` It is a non empty set of all runs.

- `Blockchain protocol:` It is denoted by P, and it is followed by all the agents in the blockchain.

  1. *Protocol for the agents:* is a function mapping agent i's local state to its actions allowed by the system.
  2. *Protocol for the environment:* It defines rules such as, which agents can act in a given global state, which messages will be transferred, what behaviour can an adversary show.

- `Asynchronous system:` It is a system in which there is no upper bound on the receiving/sending time of the transactions, or the consensus. Here the adversaries can delay the messages/transactions for any arbitrary amount of time.

- `Dishonest agents:` These are agents which knowingly or unknowingly try to corrupt the blokchain by giving their false view of the blockchain. In our synchronous simulation of the blockchain, the number of dishonest agents is limited and their behaviour is governed by the environment, this is done for the simplicity of the logical arguments discusses.

- `Set of agents:` It is defined as $1, ..., n$. It is an indexical state, that is the membership of agents may change with time.

- `Set of global state:` It is defined as $s_e, s_1, ...s_n$, where s_e is the environment state and s_1 to s_n are the states of the i-th agents. Since, the set of agents is an indexical state, hence the definition of global state must be changed to reflect that. One way to do this, is to define it as an infinite set $\mathcal{AG}$ which contains the names of all the agents which were ever been a part of the system. $\rho(r, m)$ is a set of agents in $\mathcal{AG}$ which are in ρ at a point (r,m).
  There are two indexical sets which are:-

  1. $\mathcal{A}$: set of agents currently in the system
  2. $\mathcal{H}$: set of honest agents currently in the system

  $\mathcal{H} \subseteq \mathcal{A}$
  or
  $\mathcal{H}(r, m) \subseteq \mathcal{A}(r, m) \forall A(r, m) \in R$

Propositional and Temporal Logic

The set ϕ denotes the primitive propositions. In the blockchain, they look like, $\phi =$ "X is a T-prefix of i's ledger", or "agent i is honest".

In the interpreted system $\mathcal{I} = (\mathcal{R}, \pi)$ where R is the system and pi is the interpretation, we get a truth value associated with each primitive and global state, as defined below:-

$\pi(p, s) \in \{true, false\}$

Now, we define some combinations of the primitive proposition ϕ at a point (r, m):-

- $(\mathcal{I}, r, m) \vDash p$ for a primitive proposition p iff $\pi(p, r(m)) = true$.
- $(\mathcal{I}, r, m) \vDash \phi \wedge \psi$ iff $(\mathcal{I}, r, m) \vDash \phi$ and $(\mathcal{I}, r, m) \vDash \psi$
- $(\mathcal{I}, r, m) \vDash \neg\phi$ iff $(\mathcal{I}, r, m) \nvDash \phi$

References

[1] J. Y. Halpern and R. Pass, "A knowledge-based analysis of the blockchain protocol," in *Proceedings Sixteenth Conference on Theoretical Aspects of Rationality and Knowledge, TARK 2017, Liverpool, UK, 24-26 July 2017*, ser. EPTCS, J. Lang, Ed., vol. 251, 2017, pp. 324–335. [Online]. Available: https://doi.org/10.4204/EPTCS.251.22