Multi-Agent Systems
Understanding blockchain communication using epistemic logic

June 28, 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 later subsections.

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

- `Agent's history:` It 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 a list of all agents at time t, the 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 nonempty 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:* It 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 behavior 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 who knowingly or unknowingly try to corrupt the blockchain by giving their false view of the blockchain. In our synchronous simulation of the blockchain, the number of dishonest agents is limited and their behavior 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 a 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 combinations of the primitive proposition ϕ at (r, m) point:-

- $(\mathcal{I}, r, m) \vDash p$ 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 $(\mathcal{I}, r, m) \nvDash \phi$

Standard temporal logic operators $\Box$ and $\bigcirc^{\triangle}$

- **Next:** $\bigcirc\phi = N\phi$ which is equivalent to $NB(\phi_i) = B(\phi_{i+1})$ which means ϕ will hold at the next state.
- **Globally:** $\Box\phi = N\phi$ which is equivalent to $GB(\phi) = \neg F \neg B(\phi)$ which means ϕ will hold on the entire subsequent paths.

Some combinations of the primitive proposition at a point (r,m):-

- $(\mathcal{I}, r, m) \vDash \Box\phi$ iff $(\mathcal{I}, r, m') \vDash \phi \forall m' >= m$
- $(\mathcal{I}, r, m) \vDash \bigcirc^{\triangle}\phi$ iff $(\mathcal{I}, r, m + \triangle) \vDash \phi$

Also, ϕ is valid in $\mathcal{I} = (R, \pi)$ if $\mathcal{I}, r, m) \vDash (r, m) \in (R \times N)$

Properties of the blockchain

- `Blockchain:` It is a distributed ledger, which is public to all its agents, and in which each agent has its own view of the current ledger.
- `Ledger:` It is a sequence of transactions.
  i.e. $L = (t_1, t_2, ..., t_N)$.
  $|L| = N$, where N is the length of the ledger.
- `Set T:` It contains all the possible transactions, which are commonly known as well.
  i.e. $t_i \in T$, where t_i is an element in the ledger, and T is its universal set.
- `Prefix of L:` It is defined as follows:-
  $(t_1, ..t_{N'})$ where, $N' <= N$
- `T-prefix of L:` It is defined as follows:-
  $(t_1, ..t_M)$ where, $M <= N - T$
  Notes: if $N <= T$ then the T-prefix is empty.
- `Honest agent:` The agents which have followed the protocol P since joining the blockchain up to the given time 'm'.

Properties of a run

1. **T-consistency:**
   It states that, for all times m, and $m' >= m$:-

   - If an i-th agent is honest at a time m in a run r,
     then, L' is a T-prefix of $L_i(r, m)$.
   - If a j-th agent is honest at a time m',
     then, L' is a prefix of $L_j(r, m')$.

2. $\triangle$ **weak growth:** It states that, for all times m, and $m' >= m + \triangle$:-

   - If i agent is honest at time m in the run r,
     and, j is honest at time m',
     then, $|L_j(r, m')| >= |L_i(r, m)|$.

3. **T-$\triangle$-acceptability:** It states that, for all times m, and $m' >= m$:-

   - If i agent is honest at time m in the run r,
     and, L' is a T-prefix of $L_i(r, m)$,
     and, j is honest at time $m' + \triangle$,
     then, L' is a T-prefix of $L_j(r, m' + \triangle)$.

A variant of common knowledge: $\triangle - \square$–common knowledge

To reason about the guarantees involved in the blockchain protocol, it is important to introduce the knowledge of each agent. To do that, we introduce the knowledge modal operator K_i to our language. Note that, $K_i\phi$ denotes simply that "agent i knows that ϕ."

For $K_i\phi$ to hold at a point (r, m), ϕ must hold at all points indistinguishable by i from the point (r, m):-
i.e. $(\mathcal{I}, r, m) \models K_i\phi$ iff $(\mathcal{I}, r', m') \models \phi \forall (r', m') \in \mathcal{K}_i(r, m)$.

Now, let us introduce the common knowledge operator, C. It denotes that, if there is a fixed set of agents G, common knowledge among G will hold if everyone in G knows that, everyone in G knows that, everyone in G knows that,... so on.

Hence, we add the variants of the operators, E_G and C_G to our language, which denotes, "everyone in G knows" and "it is common knowledge among the agents in G".

$(\mathcal{I}, r, m) \models E_G\phi$ iff $(\mathcal{I}, r, m) \models K_i\phi$ for all $i \in G$

$(\mathcal{I}, r, m) \models C_G\phi$ iff $(\mathcal{I}, r, m) \models E_G^n\phi$ for all $n >= 1$.

However, C_G is not sufficient in the case of an asynchronous system like a blockchain, where there is no global clock. Hence, a time-variant of common knowledge is needed, such as $\triangle$-common knowledge, where a suitable value of $\triangle$ is taken, to correspond to the assumption that the different agents' clocks are synchronized fairly closely.

Another reason for taking this variant is that we use an indexical set of honest agents. Hence, the common knowledge must be defined concerning this indexical set $\mathcal{I}$.

Now, an agent may not know that it is honest at a time m and hence may not know if it is in $\mathcal{I}$. This can happen, if there occurred a fault in the system or on the agent's side, due to which it did not follow the protocol at the previous step, and hence, is no longer honest, unknowingly, at time m. i.e.

- $i \in \mathcal{I} \not\Longrightarrow K_i(i \in \mathcal{I})$
- $i \in \mathcal{I} \not\Longrightarrow K_i(i \in \mathcal{I})$

However, $K_i(i \in \mathcal{I} \implies \phi)$ holds, which means if i knows that if it is in $\mathcal{I}$, then ϕ holds. We will denote it by $B_i^{\mathcal{I}}\phi$.

Therefore, $K_i\phi \implies B_i^{\mathcal{I}}\phi$ is valid and if i knows whether i is in $\mathcal{I}$, then $E_{\mathcal{I}}\phi$ can be easily shown to be equivalent to $\wedge_{i\in\mathcal{I}}K_i\phi$.

Now, we present more general agent-relative formulas based on [1]:-

- $(\mathcal{I}, r, m, i) \models$ T-prefix(X,L) iff X is a T-prefix of $L_i(m)$
- $(\mathcal{I}, r, m, i) \models I \in \mathcal{H}$ iff $i \in \mathcal{H}(r, m)$
- $(\mathcal{I}, r, m, i) \models \phi \wedge \psi$ iff $(\mathcal{I}, r, m, i) \models \phi$ and $(\mathcal{I}, r, m, i) \models \psi$
- $((\mathcal{I}, r, m, i) \models \neg\phi$ iff $(\mathcal{I}, r, m, i) \not\models \phi$
- $((\mathcal{I}, r, m, i) \models \Box\phi$ iff $(\mathcal{I}, r, m', i) \models \phi$ for all $m' >= m$
- $((\mathcal{I}, r, m, i) \models \bigcirc^{\triangle}\phi$ iff $(\mathcal{I}, r, m + \triangle, i) \models \phi$
- $((\mathcal{I}, r, m, i) \models K_j\phi$ iff $(\mathcal{I}, r', m', \phi) \models \phi$ for all $(r', m') \in \mathcal{K}_j(r, m)$

As we see, some of the semantics are unchanged, i.e. of conjunction, negation, and temporal operators. However, some of the primitive propositions' and knowledge operator's semantics are changed. For instance, the semantics for $K_j\phi$, is changed to $\mathcal{K}_j$, to give semantics relative to j agent. More specifically, it means that j knows that ϕ, from i's perspective if the interpretation of ϕ by j is true in all the worlds considered possible by j.
We now propose the following rules based on [1] which are mutually equivalent:-

1. P is T-$\triangle$-acceptable in context γ;
2. for all $i, j \in \mathcal{AG}$ and ledgers X,
   $i \in \mathcal{H} \wedge$ T-prefix$(X, L_i)) \implies \bigcirc^{\triangle}\Box(j \in \mathcal{H}) \implies T - prefix(X, L_j))$ is valid in $\mathcal{I}_{P,\gamma}$.
3. for all ledgers X,
   $I \in \mathcal{H} \wedge$ T-prefix$(X, L)) \implies \bigcirc^{\triangle}\Box E_{\mathcal{H}}$ (T-prefix(X, L)) is valid in $I_{P,\gamma}$.
4. for all ledgers X,
   $I \in \mathcal{H} \wedge$ T-prefix $(X, L) \implies C_{\mathcal{H}}^{\bigcirc^{\triangle}\Box}$(T-prefix$(X, L)$) is valid in $\mathcal{I}_{P,\gamma}$.

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