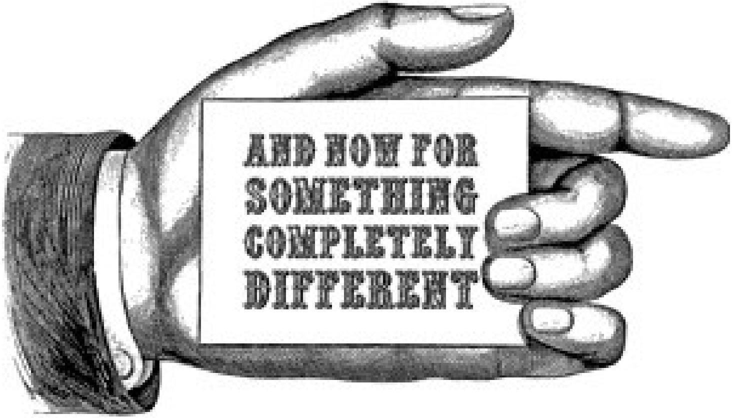
Logical Framework for Proving the Correctness of the Chord Protocol

Bojan Marinković[†], Zoran Ognjanović[†], Paola Glavan[‡]

Mathematical Institute SASA[†]
Serbia
Faculty of Mech. Engineering and Naval Architecture[‡]
Croatia
bojanm@mi.sanu.ac.rs

LAP 2018
Dubrovnik
25/09/2018


AND NOW FOR
SOMETHING
COMPLETELY
DIFFERENT

Overview

A Temporal Epistemic Logic with a Non-rigid Set of Agents for Analyzing the Blockchain Protocol

1. Motivation
2. Temporal Epistemic Logic
3. Blockchain

- Joint work with: Thomas Studer

Motivation

- Verification of distributed multi-agent systems
- System has group knowledge
- Knowledge can change during time
- Set of active agents can change during time
- Both Blockchain and Chord fit to this framework

Temporal Epistemic Logic

- Not a new thing - Halpern et al.
- Time flow is isomorphic to $\mathbb{N}$
- Set of agents is not rigid
- We proved strong completeness and syntactical proofs

Why strong completeness?

$$T = \{\mathrm{F}\neg p\} \cup \{\bigcirc^n p \mid n \in \mathbb{N}\}$$

T is unsatisfiable, but it is finitely satisfiable.

Why strong completeness?

$$T = \{\mathrm{F}\neg p\} \cup \{\bigcirc^n p \mid n \in \mathbb{N}\}$$

T is unsatisfiable, but it is finitely satisfiable.

Solution: infinite axiomatization

Temporal Epistemic Logic - Syntax (1)

- a set of agents $\mathbf{A} = \{a_1, \ldots, a_m\}$, $m \in \mathbb{N}$
- Set *For*:
  - $\neg\psi$,
  - $\phi \wedge \psi$,
  - $\bigcirc\psi$,
  - $\phi \mathtt{U} \psi$,
  - $\mathtt{K}_a\psi$,
  - $\mathtt{C}\psi$.

Temporal Epistemic Logic - Syntax (2)

- Remaining logical, temporal and knowledge connectives:
  - $\phi \vee \psi =_{def} \neg(\neg\phi \wedge \neg\psi)$,
  - $\phi \veebar \psi =_{def} (\phi \vee \psi) \wedge \neg(\phi \wedge \psi)$,
  - $\phi \rightarrow \psi =_{def} \neg\phi \vee \psi$,
  - $\phi \leftrightarrow \psi =_{def} (\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$,
  - $\mathtt{F}\psi =_{def} (\psi \rightarrow \psi)\mathtt{U}\psi$,
  - $\mathtt{G}\psi =_{def} \neg\mathtt{F}\neg\psi$,
  - $\bigcirc^0\psi =_{def} \psi$ and $\bigcirc^{n+1}\psi = \bigcirc \bigcirc^n \psi$, $n \geqslant 0$,
  - $\mathtt{E}\phi =_{def} \bigwedge_{a\in\mathbf{A}} \mathtt{K}_a\phi$, and
  - $\mathtt{E}^0\psi =_{def} \psi$ and $\mathtt{E}^{n+1}\psi = \mathtt{E}\mathtt{E}^n\psi$, $n \geqslant 0$.

Temporal Epistemic Logic - Semantics - Models (1)

Definition

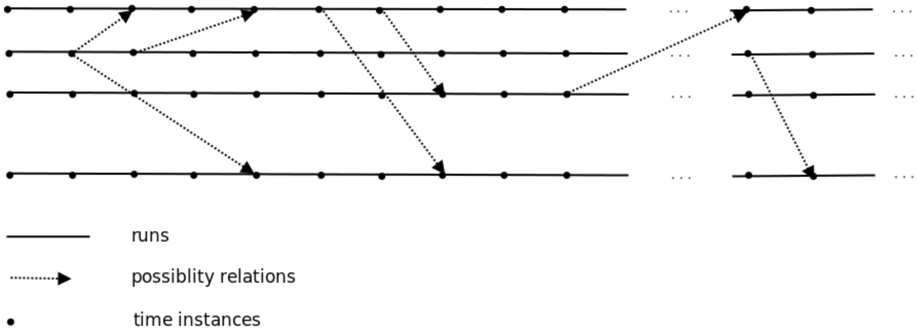
A model $\mathcal{M}$ is any tuple $\langle R, \pi, \mathcal{A}, \mathcal{K} \rangle$ such that

- R is the set of runs, where:
  - every run r is a countably infinite sequence of possible worlds r_0, r_1, r_2, ..., and
  - every possible world belongs to only one run.
- $\pi = \{\pi_i^r : r \in R\ ,\ i \in \mathbb{N}\}$ is the set of valuations:
  - $\pi_i^r(q) \in \{\top, \bot\}$, for $q \in Var$, associates truth values of propositional letters to the possible world r_i,
- $\mathcal{A}$ associates sets of active agents to possible worlds, and
- $\mathcal{K} = \{\mathcal{K}_a : a \in \mathbf{A}\}$ is the set of transitive and symmetric accessibility relations for agents, such that:
  - if $a \notin \mathcal{A}(r_i)$, then $r_i \mathcal{K}_a r'_{i'}$ is false for all $r' \in R$ and all $i' \in \mathbb{N}$.

We denote the class of all models with non rigid sets of agents by $\mathtt{Mod}_{nr}$.

Temporal Epistemic Logic - Semantics - Models (2)

- $\mathcal{K}_a(r_i)$ to denote the set of all possible worlds $r'_{i'}$ such that $r_i \mathcal{K}_a r'_{i'}$



Temporal Epistemic Logic - Semantics - Satisfiability Relation

Let $\mathcal{M} = \langle R, \pi, \mathcal{A}, \mathcal{K} \rangle$ be a model. The satisfiability relation $\models$ satisfies:

1. $r_i \models q$ iff $\pi_i^j(q) = \top$, for $q \in Var$,
2. $r_i \models \beta_1 \wedge \beta_2$ iff $r_i \models \beta_1$ and $r_i \models \beta_2$,
3. $r_i \models \neg\beta$ iff not $r_i \models \beta$ ($r_i \not\models \beta$),
4. $r_i \models \bigcirc\beta$ iff $r_{i+1} \models \beta$,
5. $r_i \models \beta_1 \mathtt{U} \beta_2$ iff there is an $s \geqslant 0$ such that $r_{i+s} \models \beta_2$, and for every k, such that $0 \leqslant k < s$, $r_{i+k} \models \beta_1$,
6. $r_i \models \mathtt{K}_a\beta$ iff $r'_{i'} \models \beta$ for all $r'_{i'} \in \mathcal{K}_a(r_i^j)$, and
7. $r_i \models \mathtt{C}\beta$ iff for every $n \geqslant 0$, $r_i \models \mathtt{E}^n\psi$

Temporal Epistemic Logic - Axiomatization

A all the axioms of the classical propositional logic

AT1 $\neg \bigcirc \beta \leftrightarrow \bigcirc \neg \beta$

AT2 $\bigcirc(\beta_1 \rightarrow \beta_2) \rightarrow (\bigcirc \beta_1 \rightarrow \bigcirc \beta_2)$

AT3 $\beta_1 \mathtt{U} \beta_2 \leftrightarrow \beta_2 \vee (\beta_1 \wedge \bigcirc(\beta_1 \mathtt{U} \beta_2))$

AT4 $\beta_1 \mathtt{U} \beta_2 \rightarrow \mathtt{F} \beta_2$

AK1 $(\mathtt{K}_i \beta_1 \wedge \mathtt{K}_i(\beta_1 \rightarrow \beta_2)) \rightarrow \mathtt{K}_i \beta_2$

AK2 $\mathtt{K}_i \beta \rightarrow \beta \mid A_a \rightarrow (\mathtt{K}_a \beta \rightarrow \beta) + A_a \rightarrow \mathtt{K}_a A_a + \neg A_a \rightarrow \mathtt{K}_a \perp$

AK3 $\mathtt{K}_i \beta \rightarrow \mathtt{K}_i \mathtt{K}_i \beta$

AK4 $\neg \beta \rightarrow \mathtt{K}_i \neg \mathtt{K}_i \beta$

AK5 $\mathtt{C} \beta \rightarrow \mathtt{E}^k \beta$, for every $k \geqslant 0$

Temporal Epistemic Logic - Inference Rules

MP from β_1 and $\beta_1 \to \beta_2$ infer β_2

RTN from β infer $\bigcirc\beta$

RKN from β infer $\mathtt{K}_i\beta$

RIU from $\Phi_k(\bigcirc^s\neg((\bigwedge_{l=0}^{i-1}\bigcirc^l\beta_1) \wedge \bigcirc^i\beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$ for all $i \geqslant 0$ infer $\Phi_k(\bigcirc^s\neg(\beta_1\mathtt{U}\beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$

RIC from $\Phi_k(\bigcirc^s\mathtt{E}^i\beta, (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$ for all $i \geqslant 0$ infer $\Phi_k(\bigcirc^s\mathtt{C}\beta, (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$

Temporal Epistemic Logic - Inference Rules

MP from β_1 and $\beta_1 \to \beta_2$ infer β_2

RTN from β infer $\bigcirc\beta$

RKN from β infer $\mathtt{K}_i\beta$

RIU from $\Phi_k(\bigcirc^s\neg((\bigwedge_{l=0}^{i-1}\bigcirc^l\beta_1)\wedge\bigcirc^i\beta_2),(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}})$ for all $i \geqslant 0$
infer $\Phi_k(\bigcirc^s\neg(\beta_1\mathtt{U}\beta_2),(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}})$

RIC from $\Phi_k(\bigcirc^s\mathtt{E}^i\beta,(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}})$ for all $i \geqslant 0$
infer $\Phi_k(\bigcirc^s\mathtt{C}\beta,(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}})$

RIU' from $\neg((\bigwedge_{l=0}^{i-1}\bigcirc^l\beta_1)\wedge\bigcirc^i\beta_2)$, for all $i \geqslant 0$, infer $\neg(\beta_1\mathtt{U}\beta_2)$

RIC' from $\mathtt{E}^i\beta$, for all $i \geqslant 0$, infer $\mathtt{C}\beta$

Nested Implication

Definition

We also define a sequence of formulas $\Phi_k(\tau, (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$ as a k-nested implications based on the sequence of formulas $(\theta_j)_{j\in\mathbb{N}}$ in the following recursive way:

- $\Phi_0(\tau, (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}}) = \theta_0 \to \tau$,
- $\Phi_{k+1}(\tau, (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}}) = \theta_{k+1} \to \mathtt{B}_k \Phi_k(\tau, (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$,

where each $\mathtt{B}_k$ is a (possible empty) sequence of alternating blocks of the operators of the forms:

- $\bigcirc^{l_i}$ and
- $\mathtt{K}_{a_{i_0}} \ldots \mathtt{K}_{a_{i_k}}$.

$$\Phi_3(\tau, (\theta_j)_{j\in\mathbb{N}}) = \theta_3 \to \mathtt{K}_{a_2}(\theta_2 \to \bigcirc^2 \mathtt{K}_{a_1} \bigcirc (\theta_1 \to (\theta_0 \to \tau)))$$

Nested Implication (cont.)

$$\Phi_{k+1}(\tau, (\theta_j)_{j\in\mathbb{N}}) = \theta_{k+1} \rightarrow \mathtt{B}_k \Phi_k(\tau, (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$$

- Why $\rightarrow$ - suitable for Deduction theorem
- Why $\mathtt{B}_k$ - for Strong Completeness theorem: if $T \vdash \alpha$ then $\bigcirc T \vdash \bigcirc\alpha$ ($\mathtt{K}_e T \vdash \mathtt{K}_e \alpha$)

Temporal Epistemic Logic - Soundness and Completeness

- Syntactical consequence
- Soundness: $\vdash \beta$ implies $\models \beta$
- Maximal consistent set
- Canonical model
- Strong completeness: Every consistent set of formulas is satisfiable

Temporal Epistemic Logic - Maximal Consistent Set

$For = \{\beta_i | i \geqslant 0\}$ - set of all formulas, T consistent set

1. $T_0 = T$,
2. If β_i is consistent with T_i then $T_{i+1} = T_i \cup \{\beta_i\}$,
3. If β_i is not consistent with T_i and has the form $\Phi_k(\bigcirc^s \neg(\beta^{'} \mathtt{U} \beta^{''}), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}}))$ then
$$T_{i+1} = T_i \cup \{\neg\beta_i, \neg\Phi_k(\bigcirc^s \neg((\bigwedge_{l=0}^{i_0-1} \bigcirc^l \beta^{'}) \wedge \bigcirc^{i_0} \beta^{''}), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})\}$$
where i_0 is a nonnegative integer such that T_{i+1} is consistent,
4. If β_i is not consistent with T_i and has the form $\Phi_k(\mathtt{C}\beta, (\theta_j)_{j\in\mathbb{N}})$ then
$$T_{i+1} = T_i \cup \{\neg\beta_i, \neg\Phi_k(\bigcirc^s \mathtt{E}^{i_0} \beta, (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})\}$$
where i_0 is a nonnegative integer such that T_{i+1} is consistent,
5. Otherwise $T_{i+1} = T_i$,
6. $T^* = \bigcup_{n\geqslant 0} T_n$.

Temporal Epistemic Logic - Canonical Model

$$\mathbb{M}^* = \langle R, \pi, \mathcal{A}, \mathcal{K} \rangle$$

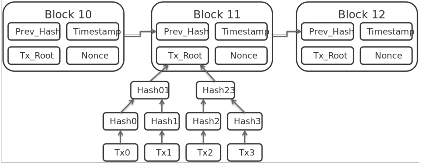
- for every $W \in \mathcal{W}$, a run is the sequence $r^W = \langle W_0, W_1, \ldots \rangle$, $(W = W_0; W_s = \{\beta : \bigcirc\beta \in W_{s-1}\}, s > 0)$, and R is a set of runs,
- for every propositional letter q, $\pi_i^{r^W}(q) = \top$ iff $q \in W_i$,
- for an agent a, $a \in \mathcal{A}(r_i)$ iff there is no formula β such that $K_a\beta \wedge K_a\neg\beta \in W_i$,
- $r_i^W \mathcal{K}_a r_{i'}^{W'}$ iff $\mathtt{K}_a^-(W_i) \subset W'_{i'}$.

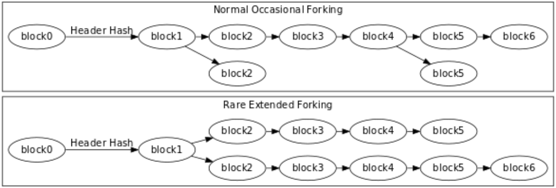
Nakamoto's Definition of Blockchain

Satoshi Nakamoto {satoshin@gmx.com; www.bitcoin.org},
`https://bitcoin.org/bitcoin.pdf`,
Bitcoin: A Peer-to-Peer Electronic Cash System, 2008

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult Proof-of-Work (PoW) for its block.
4. When a node finds a PoW, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Blockchain (2)





Temporal Epistemic Blockchain Logic - Preconditions

1. Blocks are sent across the network much faster than they are created. Every new block is received by agents in the round in which the block is produced.
2. While some messages may get lost, in every round every active agent receives at least one new block.
3. If an agent produces a new block, it adds that block to its chain.
4. Forks will be resolved after some fixed number of rounds.

Primitives

- Current round of the system $\mathbf{RND} = \{rnd_i | i \in \mathbb{N}\}$, $r_j \models rnd_i$ iff $i = j$,
- Active agent: $a^i := rnd_i \to A_a$, $a \in \mathbf{A}$ i.e., a^i ($r_i \models a^i$, if $a \in \mathcal{A}(r_i)$),
- $\mathbf{POW} = \{pow_{a,i} | a \in \mathbf{A}, i \in \mathbb{N}\}$, $pow_{a,i}$ means: a produces the proof-of-work (PoW) at the time instant i, and
- $\mathbf{ACC} = \{acc_{a,b,i} | a, b \in \mathbf{A}, i \in \mathbb{N}\}$, $acc_{a,b,i}$ means: a accepts the PoW produced at the time instant i by the agent b
- $e_{a,i} := \bigwedge_{b \in \mathbf{A}} (A_b \to acc_{b,a,i})$ - everyone accepts PoW of a produced at s

Temporal Epistemic Blockchain Logic - Axioms

AB1 $rnd_i \to \bigcirc(rnd_{i+1} \wedge \neg rnd_i)$

AB2 $rnd_i \to \bigvee_{a \in \mathbf{A}} pow_{a,i}$

AB3 $rnd_i \to \neg pow_{a,j}$, for all $i < j$

AB4 $pow_{a,i} \to a^i$

AB5 $pow_{a,i} \to \bigcirc pow_{a,i}$

AB6 $a^i \to \underline{\bigvee}_{b \in \mathbf{A}} acc_{a,b,i}$,

AB6' $rnd_j \wedge acc_{a,b,i} \to a^j$

AB7 $acc_{a,b,i} \to pow_{b,i}$

AB8 $acc_{a,b,i} \to \neg acc_{a,c,i}$, for $b \neq c$

AB9 $e_{a,i} \to \bigcirc e_{a,i}$

AB10 $(acc_{a,c,i} \wedge acc_{b,a,j}) \to acc_{b,c,i}$ for $i < j$

AB11 $acc_{a,b,i} \to \mathrm{K}_a acc_{a,b,i}$

AB12 $\neg acc_{a,b,i} \to \mathrm{K}_a \neg acc_{a,b,i}$

AB13 $rnd_i \to (\mathrm{K}_a rnd_i \wedge \mathrm{K}_a \neg rnd_j)$, for $i \neq j$

AB14 $rnd_{i+z} \to \underline{\bigvee}_{a \in \mathbf{A}} e_{a,i}$

AB15 $\neg pow_{a,i} \to \mathrm{E} \neg pow_{a,i}$

Temporal Epistemic Blockchain Logic - Properties (1)

- There cannot be agreement of acceptance of two different choices $e_{a,i} \rightarrow \neg e_{b,i}$.
- Everybody agrees on earlier proof-of-work $acc_{a,b,j} \wedge e_{a,i} \rightarrow e_{b,j}$, for $j < i$.
- All agents know what is the current round $rnd_i \rightarrow \mathtt{C} rnd_i$.
- After z number of rounds, everyone agrees on accepted proof-of-work and this agreement is common knowledge $rnd_{i+z} \wedge acc_{a,b,i} \rightarrow \mathtt{C} e_{b,i}$.
- Everyone has to accept the unique proof-of-work $\mathtt{C}(pow_{b,i} \wedge \bigwedge_{c \neq b} \neg pow_{c,i} \rightarrow e_{b,i})$.
- The active agents have unique common history up to the last z rounds: $rnd_{i+z} \rightarrow \mathtt{C} \bigwedge_{k=0}^{i} e_{a_k,k}$.

Conclusion and Future Work

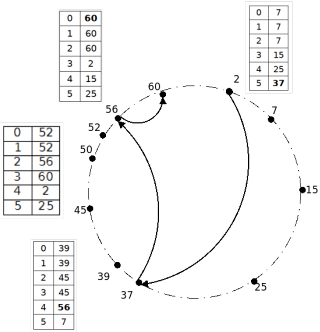
- Provided axiomatization and proved strong completeness for logic of time and knowledge with non-rigid set of agents
- Examples of usage: verification of Blockchain
- Add the probability to this logic
  (Pr+LTL;Pr+Kn;Kn+LTL) $\rightarrow$ Pr+LTL+Kn
- Verify given proof in one of the formal proof assistants
  (e.g., Coq, Isabelle/HOL)

Thank you!
Questions?

Changes of Logic

- $\mathtt{U}$ is not used
- Past operators are used $(\bullet, \mathtt{P}, \mathtt{H})$
- Common knowledge is not used

- Nodes form a ring-shaped network
- Mapping the given key onto a node using consistent hashing
- Key mapping: $hash(node) \geqslant hash(key)$
- Node is aware of only a few ($O(\log N)$) other nodes
- Periodical check of successor and predecessor
- Lookups are resolved via $O(\log N)$ messages in the worst case



Chord Specification - Definition of Correctness

- Stable pair: $n_k \Cap n_l$ at $\langle r, t\rangle$ iff chains of successor and predecessors between two nodes are "sorted"

- Stable network: $\circledcirc$ at $\langle r, t\rangle$ iff $n_k \Cap n_k$ for all $n_k \in \mathbf{N_a}$ (whole network is "sorted" - correct structure)
- Correctness with respect of "regular runs" and fairness condition

Proof of the Correctness - Main Theorem

Theorem

If the network is not stable now, in the future it will become stable:

$$\vdash \neg\circledcirc \rightarrow \mathbf{F}\circledcirc$$