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

Bojan Marinković[1], Paola Glavan[2],
Zoran Ognjanović[1], Thomas Studer[3]
[1]Mathematical Institute of the Serbian Academy of Sciences and Arts, Serbia
[bojanm,zorano]@mi.sanu.ac.rs
Faculty of Mech. Engineering and Naval Architecture[2], Croatia
pglavan@fsb.hr
University of Bern[3], Switzerland
tstuder@inf.unibe.ch

Abstract

In this paper we provide a strongly complete axiomatization of a temporal epistemic logic in which non-rigid sets of agents are allowed. Using this framework, we prove a number of properties of the blockchain protocol with respect to the given set of axioms and premises.

Keywords: multi-agent systems, blockchain, temporal epistemic logic, formal model, specification/verification.

1 Introduction

Study of epistemic and tense logics started, if not earlier, in the 1950s, 1960s with [20, 35]. Since then, reasoning about knowledge and time has been applied in many fields. Particularly, it has been proven useful in analyzing message-passing based protocols in distributed computer networks [15, 16, 17], where a suitable semantics was proposed, and modal operators are used to express both agents' knowledge and temporal properties of actions in distributed systems.

In this paper, we provide a strongly complete [1] Hilbert-style axiomatization of a temporal epistemic logic with respect to Kripke-like semantics in which the set of active agents need not be rigid, i.e., an agent may alternately become active and nonactive. This property of agents implies that knowledge does not satisfy that everything which is known is true (and in that sense it might be also called belief [15]), so a knowledge of an agent a is described using the modal operator $\mathtt{K}_a$, that is interpreted with a symmetric and transitive indistinguishability (accessibility) relation, while the temporal part of the logic is discrete

[1] "every consistent set of formulas is satisfiable", in contrast to weakly complete—"every consistent formula is satisfiable"

linear time (future) LTL logic, where the flow of time is isomorphic to the natural numbers, and the corresponding part of the formal language contains the operators Next ($\bigcirc$) and Until ($\mathtt{U}$). The epistemic part is formalized using the multi-agent modal logic KB4 (since reflexivity is not required) with addition of axioms and rules for common knowledge (denoted by the operator $\mathtt{C}$), and for the temporal part we follow the approach presented in [31]. We consider two variants of our temporal epistemic logic. In the first one, we extend our formal language so that, if the set of agents is non rigid, it is possible to reason about knowledge of active agents. In the second logic, we deal with rigid sets of agents and one of the standard characteristics of knowledge which says that agents know only true facts. In that case accessibility relations should also be reflexive. We provide complete axiomatizations for those systems.

We have already mentioned weak and strong completeness that connect the syntactic and the semantic notions of consistency and satisfiability. Obviously, weak completeness follows trivially from the strong one, but the opposite direction is not straightforward. Here the notion of compactness ("a set of formulas is satisfiable iff every finite subset of it is satisfiable") plays an important role. For logics that fulfill compactness for every set of formulas, strong completeness is a consequence of weak completeness (e.g., in classical logic). However, there are logics where compactness fails, and there are unsatisfiable sets of formulas that are finitely satisfiable ("every finite subset is satisfiable"). Actually, both the temporal logic LTL and the epistemic logic are not compact. In case of non-compact logics, strong completeness does not follow from the weak one. Namely, having a finitary (i.e., recursive) sound and weakly complete axiomatic system, it is not possible to prove inconsistency of an unsatisfiable, but finitely satisfiable, set F of formulas, because every finite proof uses only finite number of formulas from F, every finite subset of F is satisfiable, and, by soundness, cannot be proven inconsistent. To avoid that logical obstacle, we provide here an axiomatization containing infinitary inference rules (with countable many premises and one consequence), which, because of strong completeness, guarantee that every unsatisfiable set of formulas is inconsistent. We emphasize that in this paper the term infinitary concerns the meta language only, i.e., the object language is countable, and formulas are finite, while proofs are allowed to be infinite.

Nowadays, one of the most popular distributed protocols is the blockchain protocol [30], which is used, for example, to synchronise copies of the public ledger in the bitcoin cryptocurrency. In the formal language of our logic we formulate a theory related to the definition of blockchain and illustrate the expressiveness of the logic by reasoning about properties of the protocol.

The main contributions of this paper are:

- we present a temporal epistemic logic in which the set of active agents is allowed to change over time,
- we present the corresponding infinitary axiomatization and prove its strong completeness with respect to a class of Kripke-like models, and

- to illustrate the expressiveness of the presented formal language, we provide a description of the synchronous version of the blockchain protocol as a theory in the logic.

Finally, we note that, although we consider only propositional logic in this paper, our approach can be extended to the first order case. It is well known that in case of some first order logics (e.g., first order dynamic logic [11], first order LTL [38], first order probability logic [1], etc.), there are no sound and complete finitary axiomatic systems. However, strongly complete axiomatization can be obtained by adding infinitary inference rules [12, 31, 33].

1.1 Related work

Temporal and epistemic logics are broadly analyzed in the literature. Here we will mention some of the relevant papers and books. John Burgess [8] discussed a propositional temporal language with the operators Since and Until introduced in [22], and presented weak completeness proofs for a number of classes of temporal models. The ability to describe properties of programs using the future-time linear discrete temporal logic LTL with the operators $\bigcirc$ and $\mathtt{U}$ particularly focused research on it [25]. The paper [24] gave a comprehensive analysis of propositional LTL (also including the past operators Previous and Since) and provided a weakly complete axiomatization. The paper [37] was the first proposing an infinitary Prawitz-type natural deduction system for propositional LTL with the operators $\bigcirc$ and Always ($\mathtt{G}$). The proposed infinitary rule

$$\{\bigcirc^{n+k}A \ : \ k = 0, 1, 2, \ldots\} \vdash \bigcirc^{n}\mathtt{G}A$$

can be intuitively read as "(in every future time instant) if A holds, and A holds in the next time instant, and in the time instant after it, etc., then A always holds".

The books [15, 28] gave systematic overviews of the field of epistemic logic. To characterize properties of knowledge they used finitary axiomatizations based on modal systems $S5$ and $KD45$. In [15] infinitary nature of common knowledge was captured using finitary Induction inference rule

$$A \to \mathtt{E}_G(B \wedge A) \vdash A \to \mathtt{C}_G B,$$

where $\mathtt{E}_G$ denotes that everyone in the group G knows. In [36] temporal, epistemic and dynamic propositional modal logics with infinitary inference rules were discussed. The logics were given in the form of natural deduction systems with infinitary sets of premises in inference rules while proof trees remained finite. The paper also justified the need for such infinitary rules by noting the above mentioned compactness issue. Completeness proofs for the considered logics were given. A particular example was the epistemic logic with common knowledge characterized with the following infinitary rule

$$\{\mathtt{K}_{a_0} \ldots \mathtt{K}_{a_{k-1}}A \ : \ k = 0, 1, 2, \ldots, \ a_i's \text{ are agents } \} \vdash \mathtt{C}A.$$

The paper [23] proposed several formal systems to describe combinations of knowledge, belief and time, but did not find the corresponding classes of models for which the systems are complete. In [15] an interaction of knowledge and time was considered and finitary weakly complete axiomatization was provided. Finitary axiomatizations for a number of discrete linear time temporal epistemic logics were given in [19]. The temporal part of the formal language contains $\bigcirc$ and $\mathtt{U}$, while the epistemic part covers the cases of a single agent, and of multiple agents with common knowledge. Several properties of agents were discussed and, while some of them cannot be recursively axiomatized, finitary axiomatic systems were given to the other ones using the above mentioned Induction rule. One of usual assumptions in temporal epistemic framework is that the set of agents is rigid (all agents are active during any execution of a protocol), but the paper [18] considers also sets of agents that are non-rigid, i.e., agents can temporarily switch from active to inactive and vice versa.

On the other hand, there are not many papers providing formal logical analysis of the blockchain protocol. In [5] a dynamic logic BCL was introduced to describe how an agent's knowledge is changed when a new block that might be added to the blockchain arrives. The paper [18] presented a model-theoretic approach to address the issue of achieving consensus on a public ledger implemented as a blockchain, where it is allowed that some of the agents can enter and leave the network. The paper used some variants of common knowledge (i.e., Δ-, and Δ-$\Box$-common knowledge) that rely on the assumption that agents' local clocks can be synchronized reasonably closely—with a delay of Δ time instants. A probabilistic extension of this approach (e.g., "what is the probability that a transaction is in a ledger?") is also discussed in [18].

The papers [10, 34] considered the blockchain protocol from a cryptographic perspective. They are interested in possible influences of adversaries to the protocol consistency. The paper [10] gave a probabilistic analysis of blockchain assuming that the number of agents in a network remain fixed and that agents are synchronized (which can be also understood as the requirement that time is divided in such a way that messages are always instantly delivered without delays). It was proved that with a high probability any two honest agents have a large common prefix, and that in a chain of an honest agent the ratio of blocks produced by adversaries are small. On the other hand, [34] argued that synchronicity of a network is an unrealistic assumption, and applied its analysis to an asynchronous setting. Assuming also a possibility that new agents join a network while an instance of the blockchain protocol runs, the paper proved generalization of the properties given in [10]. [34] also noticed that synchronous protocols can be considered as Δ-delayed protocols, and that one could restrict its focus on synchronous protocols as far as crypto-properties (like proof-of-work) are not discussed.

1.2 Plan of the paper

The rest of the paper is organized as follows. In Section 2 we describe syntax, semantics and an axiomatic system for the considered temporal epistemic logic.

Section 3 introduces the basics of the blockchain protocol and provides a theory (a set of proper axioms). Relying on the presented strongly complete axiomatization we prove a number of properties of the protocol. Section 4 contains concluding remarks and directions for further work. In Appendix A a proof of strong completeness of the presented axiomatization is given.

2 Temporal Epistemic Logic

2.1 Syntax

Let $\mathbb{N}$ be the set of nonnegative integers, Var a nonempty at most countable set of propositional letters, and $\mathbf{A} = \{a_1, \ldots, a_m\}$, where $m \in \mathbb{N}$, a set of agents. The set For of all formulas is the smallest superset of Var which is closed under the following formation rules:

- $\psi \mapsto *\psi$ where $* \in \{\neg, \bigcirc, \mathtt{K}_a, \mathtt{C}\}$, where $a \in \mathbf{A}$,
- $\langle \phi, \psi \rangle \mapsto \phi * \psi$ where $* \in \{\wedge, \mathtt{U}\}$.

The operators $\neg$ and $\wedge$ represent standard logical negation and conjunction. The operators $\bigcirc$ and $\mathtt{U}$ are standard temporal operators Next and Until. The operator $\mathtt{K}_a$ is read "agent a knows", while $\mathtt{C}$ denotes common knowledge. Theories are sets of formulas.

The remaining logical, temporal and knowledge connectives $\vee$, $\veebar$, $\rightarrow$, $\leftrightarrow$, $\mathtt{F}$, $\mathtt{G}$, $\mathtt{E}$ are defined in the usual way:

- $\phi \vee \psi =_{def} \neg(\neg\phi \wedge \neg\psi)$,
- $\phi \veebar \psi =_{def} (\phi \vee \psi) \wedge \neg(\phi \wedge \psi)$,
- $\phi \rightarrow \psi =_{def} \neg\phi \vee \psi$,
- $\phi \leftrightarrow \psi =_{def} (\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$,
- $\mathtt{F}\psi =_{def} (\psi \rightarrow \psi)\mathtt{U}\psi$,
- $\mathtt{G}\psi =_{def} \neg\mathtt{F}\neg\psi$,
- $\bigcirc^0\psi =_{def} \psi$ 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 $\mathtt{E}^{n+1}\psi = \mathtt{E}\mathtt{E}^n\psi$, $n \geqslant 0$.

We also define a sequence of formulas

$$\Phi_k(\tau, (\theta_j)_{j \in \mathbb{N}}, (\mathtt{B}_j)_{j \in \mathbb{N}})$$

as 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
- $\mathtt{K}_{a_0} \dots \mathtt{K}_{a_{i_k}}$.

For example,

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

This definition follows the form of the probabilistic k-nested implications presented in [29, 39] and also of AF-programs from [2]. Formulas of this form are used to formulate infinitary inference rules that are essential in the presented axiomatization. The need of k-nested implications in inference rules comes directly from our completeness proof where they give a form of deep inference that is essentially the same as nested sequents [3]. Deep inference refers to deductive systems in which rules can not only be applied to outermost connectives but also deep inside formulas.

2.2 Semantics

In this paper we will consider time flow which is isomorphic to the set $\mathbb{N}$. Since we are dealing with a multi-agent system where agents have to share knowledge, the obvious choice is to use the logic of time and knowledge, where models are propositional Kripke structures with possible worlds (i.e., possible worlds are classical propositional models) that are essentially interpreted systems from [15].

Definition 1. *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 to propositional letters of 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* $\mathtt{Mod}_{nr}$.

We will use $\mathcal{K}_a(r_i)$ to denote the set of all possible worlds $r'_{i'}$ such that $r_i \mathcal{K}_a r'_{i'}$. We mentioned above that our aim is to formalize systems in which sets of active agents need not be rigid, which means that an agent a may be active in some possible world r_i and not active in some other r'_m. This property is formalized using the function $\mathcal{A}$. Note that, if an agent a is not active in a world r_i, there is no world (including r_i itself) accessible from r_i by $\mathcal{K}_a$. In the terminology of the modal logics community such world is called dead end (wrt. the agent a). The idea that $r_i \mathcal{K}_a r'_{i'}$ implies that $a \in \mathcal{A}(r_i)$ can be traced back at least to [13], where it is explained that "this restriction is reasonable because we do not want to ascribe knowledge to an agent at any world where he is not present". We will return to this after introducing the satisfiability relation in Definition 2.

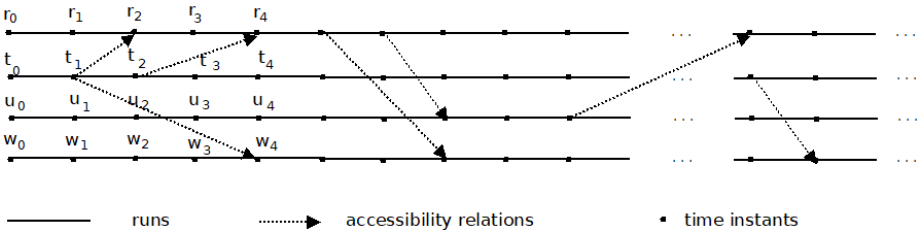

Figure 1: Kripke model

Figure 1 illustrates a model which contains the runs r, t, u and w, where r is the sequence r_0, r_1, r_2, ..., and similarly for the other runs. In this model, for example, $t_1 \mathcal{K}_1 r_2$, etc.

2.3 Satisfiability relation

The satisfiability relation $\models$ on possible worlds and formulas is recursively defined as follows:

Definition 2. *Let* $\mathcal{M} = \langle R, \pi, \mathcal{A}, \mathcal{K} \rangle$ *be an* $\mathtt{Mod}_{nr}$ *model. The satisfiability relation* $\models$ *satisfies:*

1. $r_i \models q$ *iff* $\pi_i^r(q) = \top$, *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* $j \geqslant 0$ *such that* $r_{i+j} \models \beta_2$, *and for every* k, *such that* $0 \leqslant k < i$, $r_{j+k} \models \beta_1$,

6. $r_i \models \mathtt{K}_a\beta$ *iff* $r'_{i'} \models \beta$ *for all* $r'_{i'} \in \mathcal{K}_a(r_i)$, *and*

7. $r_i \models \mathtt{C}\beta$ *iff for every* $n \geqslant 0$, $r_i \models \mathtt{E}^n\psi$. □

A set of formulas is satisfiable if there is a possible world r_i of a run r in a model $\mathcal{M}$ such that every formula from the set holds in r_i. A formula α is satisfiable if the set $\{\alpha\}$ is satisfiable. A formula is valid ($\models \alpha$) if it holds in every r_i in each model. A formula α is a semantic consequence of a set of formulas F ($F \models \alpha$) if there is no model $\mathcal{M}$ with a possible world r_i such that every formula from F holds in r_i but α does not hold in r_i.

Note that $r_i \models \mathtt{E}^k\beta$ means:

- if $k = 0$, $r_i \models \beta$,
- if $k = 1$, $r_i \models \wedge_{a\in\mathbf{A}}\mathtt{K}_a\beta$,
- if $k = 2$, $r_i \models \wedge_{a\in\mathbf{A}}\mathtt{K}_a\mathtt{E}\beta$, i.e., $r_i \models \wedge_{a\in\mathbf{A}}\wedge_{b\in\mathbf{A}}\mathtt{K}_a\mathtt{K}_b\beta$, i.e., $r_i \models \wedge_{a,b\in\mathbf{A}}\mathtt{K}_a\mathtt{K}_b\beta$, etc.

In other words, $\mathtt{E}^k\beta$ is satisfied in r_i iff every formula of the form $\mathtt{K}_{a_{i_1}} \ldots \mathtt{K}_{a_{i_k}}\beta$, for $a_{i_l} \in \mathbf{A}$, is satisfied in r_i. It follows that $\mathtt{C}\beta$ is satisfied in r_i iff for every k every formula of the form $\mathtt{K}_{a_{i_1}} \ldots \mathtt{K}_{a_{i_k}}\beta$ is satisfied in r_i.

Since we consider models with non rigid sets of active atoms, if $a \notin \mathcal{A}(r_i)$, we have that $r_i \models \mathtt{K}_a\beta$, for every formula β. So, it may happen that an agent knows something that is not true, which implies that the well known property $\mathtt{K}_a\beta \rightarrow \beta$ is not valid. However, since satisfiability of knowledge of a group is represented as a conjunction of knowledge of agents from the group, the fact that non active agents know everything does not affect knowledge of the group. In other words, a group of agents knows β if and only if β is known by active agents.

Following the above definitions, it can be seen that the operators $\mathtt{F}$ and $\mathtt{G}$ intuitively mean "eventually true in the future" and "always true in the future", respectively. Also, note that in this paper we use the reflexive, strong version of the until operator, so that if $\alpha\mathtt{U}\beta$ holds, then β must eventually hold, while "the future includes the present" which means that:

- $r_i \models \mathtt{F}\beta$ iff there is $k \geqslant 0$ such that $r_{i+k} \models \beta$, and
- $r_i \models \mathtt{G}\beta$ iff for every $k \geqslant 0$, $r_{i+k} \models \beta$.

Now we can now give two finitely satisfiable sets of formulas that are unsatisfiable [36, 37] ($p \in Var$):

- $F_1 = \{\neg\mathtt{G}p\} \cup \{\bigcirc^n p \ : \ n \in \mathbb{N}\}$, and
- $F_2 = \{\neg\mathtt{C}p\} \cup \{\mathtt{E}^n p \ : \ n \in \mathbb{N}\}$.

For example, the set F_1 intuitively says that p holds in every particular future time instant, yet p does not always hold in the future. It follows from our completeness theorem that these sets are inconsistent wrt. our proof system. As we mentioned above, inconsistency of these sets cannot be proved wrt. any finitary proof systems.

2.4 Other classes of models

It is well known that the class $\mathtt{Mod}_{nr}$ of models characterizes a weaker form of knowledge—belief. So, to reason about knowledge of agents we will also consider two other classes of models. The first class corresponds to situations in which everything that agents know is true:

Definition 3. *The class* $\mathtt{Mod}_r$ *of models contains all* $\mathtt{Mod}_{nr}$*-models which satisfies that the set of active agents is rigid and that all* $\mathcal{K}_a$ *are equivalence relations, i.e., that:*

- $\mathcal{A}(r_i) = \mathbf{A}$*, for every possible world* r_i*, and*
- $\mathcal{K} = \{\mathcal{K}_a : a \in \mathbf{A}\}$ *is the set of reflexive, transitive and symmetric accessibility relations.*

In the second case, we have first to introduce a set of new propositional letters: A_a, for every $a \in \mathbf{A}$, with the intended meaning that an A_a holds in a possible world iff the agent a is active in that world:

- if r_i is a possible world in a model $\mathcal{M}$, $r_i \models A_a$ iff $a \in \mathcal{A}(r_i)$.

The second class consists of $\mathtt{Mod}_{nr}$-models that satisfy an additional condition. We denote this class by $\mathtt{Mod}_{nr+}$ and define it as follows.

Definition 4. *The class* $\mathtt{Mod}_{nr+}$ *of models contains all* $\mathtt{Mod}_{nr}$*-models that satisfy:*

- *if* $a \in \mathcal{A}(r_i)$*, then* $r_i \mathcal{K}_a r_i$*.*

It is well known that in models from the class $\mathtt{Mod}_r$ everything that agents know is true. Note that the same holds in $\mathtt{Mod}_{nr+}$-models for active agents. Also, note that for $\mathtt{Mod}_{nr+}$-models the following holds: if $r_i \models A_a$ and $r_i \mathcal{K}_a r'_{i'}$, then $r'_{i'} \models A_a$. Otherwise, if $r'_{i'} \not\models A_a$, then it is not $r'_{i'} \mathcal{K}_a r_i$, which contradicts our assumption about symmetry of $\mathcal{K}_a$.

The satisfiability relation for the new classes of models can be defined in the same way as above. In the rest of the paper, if the context is not clear, we will use the subscripts so that $\models_{nr}$, $\models_{nr+}$ and $\models_r$ denote the corresponding satisfiability relations.

Models from the class $\mathtt{Mod}_{nr+}$ will be used to describe the blockchain protocol in Section 3.2.

2.5 Axiomatization

The axiomatic system $\mathtt{Ax}_{nr}$ contains the following axiom schemata (AT and AK for axioms about time and knowledge, respectively):

A all the axioms of the classical propositional logic

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

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

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

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

AK1 $(\mathtt{K}_a\beta_1 \wedge \mathtt{K}_a(\beta_1 \to \beta_2)) \to \mathtt{K}_a\beta_2$

AK3 $\mathtt{K}_a\beta \to \mathtt{K}_a\mathtt{K}_a\beta$

AK4 $\mathtt{K}_a\neg\beta \to \mathtt{K}_a\neg\mathtt{K}_a\beta$

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

and inference rules (RTN and RKN for necessitation for time and knowledge, respectively; RIU and RIC denote the infinitary rules related to until and common knowledge):

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

RTN from β infer $\bigcirc\beta$

RKN from β infer $\mathtt{K}_a\beta$

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 $\Phi_k(\bigcirc^s\mathtt{C}\beta, (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$.

[AT1–AT4] are axioms of LTL (see [24]), while [AK1, AK3, AK4, AK5] are the usual modal axioms used for reasoning about knowledge (see [15]) in the case of non-rigid set of agents (the set of agents that are active may change). If the set of agents is rigid, we should include an additional, so-called Knowledge axiom:

AK2 $\mathtt{K}_a\beta \to \beta$

which implies reflexivity of the accessibility relations $\mathtt{K}_a$. It is also possible to talk about knowledge of an agent a (non)active in a possible world using the following axioms that generalize [AK2]:

AK2' $A_a \to (\mathtt{K}_a\beta \to \beta)$,

AK2'' $A_a \to \mathtt{K}_aA_a$, and

AK2''' $\neg A_a \to \mathtt{K}_a\bot$.

We will show that, in the presence of [AK2'], [AK2''] and [AK2'''], the accessibility relation $\mathcal{K}_a$ satisfies that if $a \in \mathcal{A}(r_i)$, then $r_i\mathtt{K}_ar_i$. Note that, we have as a consequence of [AK2'] and [AK2'''] that $\mathtt{K}_aA_a$ holds.

The rule [MP] is modus ponens, [RTN] and [RKN] resemble necessitation, while [RIU] and [RIC] are infinitary inference rules that characterize the Until

operator, and the common knowledge operator, respectively. These rules are given in terms of k-nested implications, similarly as in [29, 39]. The structure of [RIU] and [RIC] stems from our completeness proof and is more-or-less the same as the structures of the rule of intersection [2], and of the infinitary nested sequent rules for common knowledge in [6] and greatest fixed points in [7]. In our present paper, deep inference is needed to obtain strong completeness in the context of knowledge and time whereas in [6] and [7] deep inference was essential to achieve syntactic cut-elimination for modal fixed point logics. In cases when every θ_j is $p \vee \neg p$, every $\mathtt{B}_j$ is an empty sequence of operators, and $s = 0$, the infinitary rules have the following simpler forms:

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 $\mathtt{C}\beta$.

For example, [RIU'] intuitively means that if there is no future time instant in which β_2 holds, such that β_1 holds in all time instants between the current time instant and the one in which β_2 holds, then $\beta_1 \mathtt{U} \beta_2$ does not hold in the current time instant. Similarly, [RIC'] says that we if have $\mathtt{E}^i \beta$ for all i, then we can deduce that β is common knowledge.

We will use:

- $\mathtt{Ax}_{nr+}$ to denote $\mathtt{Ax}_{nr}+$ Axioms [AK2', AK2'', AK2'''], and
- $\mathtt{Ax}_r$ to denote $\mathtt{Ax}_{nr}+$ Axiom [AK2].

2.6 Soundness and Completeness

In this part we will state that our systems are sound and complete with respect to the corresponding classes of models. Informally speaking, soundness means that we cannot prove anything that is false, and (so-called weak) completeness means that we can prove everything that is true. However, in the sequel we will prove a stronger version of completeness, so-called strong completeness, which says that every consistent set is satisfiable (or equivalently that every semantic consequences of set of formula can be deduced from that set using the above axioms and inference rules). As it was mentioned in the Introduction, all proofs of the theorems from this section will be given in Appendix A. Similarly as above, we will use subscripts nr, $nr+$ and r to clarify the context, if necessary.

The inference relation $\vdash$ is defined as follows:

Definition 5. *We say that β is syntactical consequence of a set of formulas F (or that β is deducible or derivable from F) and write $F \vdash \beta$ iff there is a sequence $\beta_0, \ldots, \beta_{\lambda+1}$ (where λ is a finite or countable ordinal) such that:*

- *$\beta_{\lambda+1} = \beta$, and*
- *every β_i, $i \leq \lambda + 1$, is an axiom-instance, or $\beta_i \in F$, or β_i is derived by an inference rule applied on some previous members of the sequence.*

A formula β is a theorem ($\vdash \beta$) if it is deducible from the empty set. The rules [RTN] *and* [RKN] *can be applied only to theorems. A proof for β from F is the corresponding sequence of formulas.*

Note that the length of a proof is a countable successor ordinal.

Definition 6. *A set F is inconsistent iff $F \vdash \bot$, otherwise it is consistent. A set F of formulas is maximal if for every formula β either $\beta \in F$ or $\neg\beta \in F$. A set F is deductively closed if for every formula β, if $F \vdash \beta$, then $\beta \in F$.*

Theorem 1. *[Soundness for $\mathtt{Ax}_{nr}$] $\vdash_{nr} \beta$ implies $\models_{nr} \beta$.*

Theorem 2. *Every $\mathtt{Ax}_{nr}$-consistent set of formulas F can be extended to a maximal $\mathtt{Ax}_{nr}$-consistent set F^*.*

Theorem 3. *[Strong completeness for $\mathtt{Ax}_{nr}$] Every $\mathtt{Ax}_{nr}$-consistent set of formulas has a $\mathtt{Mod}_{nr}$-model.*

Theorem 4. *$F \models_{nr} \beta \leftrightarrow F \vdash_{nr} \beta$.*

Theorem 5. *[Soundness and Strong completeness for $\mathtt{Ax}_{nr+}$ and $\mathtt{Ax}_{r}$] The axiomatic system $\mathtt{Ax}_{nr+}$ is sound and strongly complete wrt. the class of $\mathtt{Mod}_{nr+}$-models.*

The axiomatic system $\mathtt{Ax}_{r}$ is sound and strongly complete wrt. the class of $\mathtt{Mod}_{r}$-models.

In the proofs of the completeness theorems we follow the Henkin procedure: we first prove the deduction theorem, some auxiliary statements, and Lindenbaum's theorem (which guarantees that every consistent set of formulas can be extended to a maximal consistent set), and then demonstrate how a canonical model can be obtained using maximal consistent sets of formulas. Finally, we show that the considered consistent set of formulas is satisfied in the canonical model.

3 Blockchain Protocol

In this section we will present a theory (a set of proper axioms) of our temporal epistemic logic to describe (a simplified version of) the blockchain protocol [4, 10, 30, 34]. The protocol is used to achieve consensus in distributed environments, for example as the base for bitcoin protocol, or some other cryptocurrency protocol, Byzantine agreement, the notion of a public transaction ledger, smart contracts, etc.

The following properties particularly contribute to the popularity of the blockchain protocol:

- It is managed autonomously, without third authority.

- It removes the possibility of infinite reproducibility from a digital asset, i.e., it confirms that each unit of value was transferred only once, solving the long-standing problem of double spending.
- It can assign title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

3.1 Overview of the Blockchain Protocol

The blockchain protocol can be seen as a value-exchange protocol. It allows permanent recording of verifiable transactions in a distributed network. A transaction describes a transfer of the ownership of a property from one owner to another one. Upon executing transactions, the corresponding (time stamped) transactions' data organized in blocks are added in a change-sensitive manner at the end of a decentralized, distributed and public digital ledger (also called blockchain, or chain). To achieve consensus about the accepted blocks, the nodes in the network create so-called proofs-of-work, i.e., they try to solve the unique (hard to answer, but easy to verify) hash puzzle of a new block. The first node with a valid solution (accepted by the majority of nodes) is the winner and its block is added. The ledger represents the complete history of all approved transactions. It is immutable and ordered, and records cannot be altered retroactively, without the alteration of all subsequent blocks and the consensus of the network. Hashing is used to store transaction data, so that nodes compare hash values instead of pieces of their copies of the ledger, which allows nodes to verify and check transactions inexpensively and easily.

The blockchain protocol was introduced in the following way (quotation from [30]):

> 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 for its block.
> 4. When a node finds a proof-of-work, 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.
>
> Nodes always consider the longest chain, i.e., the one containing the most proofs-of-work, to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when

the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

The above described steps (1 – 6) of the protocol execution form a round. At any round, each node attempts to increase the length of its own chain by mining for a new block: upon receiving some record m, it picks a random string and checks whether the string is a valid proof-of-work (aka "cryptographic puzzle") with respect to m and a pointer to the last block of its current chain. If so, the node extends its own local chain and broadcast it to the all the other nodes. It is possible that several chains arrive approximately simultaneously in a run of the protocol. In that case, each node chooses one of them, and works on it (approximately half choose the first one, and the other half the second one), keeping the other chains. This situation is called a fork. Forks are resolved in later rounds when a new proof-of-work is found and one branch becomes longer; the nodes that were working on the other (now shorter) branches will then switch to the longer one.

We consider the blockchain protocol that runs in a synchronous setting. We do not consider cryptographic properties of the protocol, and we assume that all nodes in the network are perfectly honest and reasonable, and that there are no dishonest nodes trying to exploit cryptographic vulnerabilities of the protocol to gain benefits.

3.2 Temporal Epistemic Blockchain Logic

In this section we will use previously introduced notions and results related to strongly complete axiomatization of the class of $\mathtt{Mod}_{nr+}$-models. We start with some notational conventions. In the rest of this section we will use the word *agent* (more frequently used in the logic community) instead of *node*. The set of agents need not to be rigid, i.e., agents are allowed to switch from active to inactive and vice versa. A situation in which different subgroups of agents add different blocks to the ledger and continue to work with them will be called *fork*, while the word *history* will serve instead of *ledger*.

In our model we describe a run of the blockchain protocol by a linear time logic-model with the set of time instants isomorphic to the set of non-negative integers. However, the meaning of time instants i, $i+1$, etc. is "the ith round", "the $i+1$st round of an execution of the protocol", etc. A round involves the following steps performed by active agents:

- agents try to find a proof-of-work for the next block,
- agents broadcast their solutions (blocks) to other agents,
- agents receive those messages, each agent accepts one of the proposed blocks and add it to its chain.

Note that in real applications the lengths of rounds of an execution of the protocol might vary, but we abstract this and only require that rounds are linearly ordered.

In this paper we assume several constraints to the original execution scenario of the protocol, since we consider blockchain protocol that runs in a synchronous setting:

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.

The assumption that broadcasting is much faster than creating new proof-of-work does hold for the Bitcoin protocol [30]. The average time until an agent receives a new block is 6.5 seconds whereas the next block will be only produced after 10 minutes (on average) [9]. Therefore, in our model, in one round at least one (but maybe several) proof-of-work are produced, they are immediately broadcasted, and each agent accepts one of them. Then the next round starts and next proofs-of-work are computed. The assumption that forks will be resolved after some fixed number of rounds is a simplification of actual blockchain implementations. In the Bitcoin protocol, we only have the following, see [14, 30]:

- Let z be the number of blocks validated by the honest agents and let $P(z)$ be the probability that an attacker will win a double spend race (i.e., to succeed to spend the same money more than once) to replace the blocks of the blockchain.
- Then $P(z)$ tends exponentially to 0 as z increases.

Hence, in practice, we only have that forks will be resolved with some (high) probability.

The assumption of synchronicity of the considered networks is used in [10]. The paper [18] discusses networks with a Δ-bounded delays, but [34] explains that every synchronous protocol can be seen as a Δ-delayed (i.e., agents are required to wait certain period). So, in case when all agents are considered honest, and there are no adversaries to benefit from Δ-times increasing of their computational power, the assumption about asynchronicity can be neglected.

We will now introduce a formal theory for our blockchain model. Since we want to reason about knowledge of agents that can alternately become active and nonactive, as the base logic we will use the one axiomatized by $\mathtt{Ax}_{nr+}$, and we consider models from the class of $\mathtt{Mod}_{nr+}$.

We define:

- $\mathbf{POW} = \{\mathsf{pow}_{a,i} | a \in \mathbf{A}, i \in \mathbb{N}\}$ is a set of atomic propositions, with the intended meaning of $\mathsf{pow}_{a,i}$ that the agent a produces a proof-of-work for round i, and

- $\mathbf{ACC} = \{\mathsf{acc}_{a,b,i} | a, b \in \mathbf{A}, i \in \mathbb{N}\}$ is a set of atomic propositions, with the intended meaning of $acc_{a,b,i}$ that the agent a accepts the proof-of-work produced for round i by the agent b.

We set

$$e_{a,i} \;:=\; \bigwedge_{b \in \mathbf{A}} (A_b \to \mathsf{acc}_{b,a,i})$$

The formulas $e_{a,i}$ mean that every active agent accepts the proof-of-work produced for round i by agent a.

Further we set

$$\mathsf{ech}_{b,i} \;:=\; \bigvee_{a \in \mathbf{A}} \mathsf{acc}_{b,a,i}$$

The formula $\mathsf{ech}_{b,i}$ means that agent b accepts some proof-of-work produced for round i.

We will use $\mathsf{z} \in \mathbb{N}$ for the fixed number of rounds after which forks are resolved.

Our theory of the blockchain protocol consists of the following proper axioms (let a, b and c denote agents from $\mathbf{A}$):

AB1 $\bigvee_a A_a$

AB2 $\mathsf{acc}_{b,a,i} \to \mathsf{pow}_{a,i}$

AB3 $\mathsf{acc}_{b,a,i} \to \mathtt{K}_b \mathsf{acc}_{b,a,i}$

AB4 $\mathsf{acc}_{b,a,i} \to \neg \mathsf{acc}_{b,c,i}$, for each $c \neq a$

AB5 $\mathsf{acc}_{a,c,j} \wedge \bigcirc \mathsf{acc}_{b,a,i} \to \bigcirc \mathsf{acc}_{b,c,j}$, for $j < i$

AB6 $A_b \wedge \bigvee_a \mathsf{pow}_{a,i} \to \mathsf{ech}_{b,i}$

AB7 $\mathsf{ech}_{a,i} \to A_a$

AB8 $\mathsf{ech}_{a,i+1} \to \mathsf{ech}_{a,i}$

AB9 $\mathsf{ech}_{b,i} \to \bigcirc \bigvee_a \mathsf{pow}_{a,i+1}$

AB10 $\neg \mathsf{ech}_{a,i} \to \neg \bigcirc \mathsf{pow}_{a,i+1}$

AB11 $\mathsf{ech}_{a,i+\mathsf{z}} \wedge \mathsf{acc}_{a,b,i} \to e_{b,i}$

The theory of the blockchain protocol not only contains the above axioms, but also their $\bigcirc$- and $\mathtt{E}$-closures, i.e., we can prefix the formulas with any number of $\bigcirc$- and $\mathtt{E}$-operators. That basically means the formulas always hold and they are common knowledge among the participants of the blockchain.

Let us briefly discuss the meaning of the above axioms.

AB1 There is always at least one agent active.

AB2 One can only accept proof-of-work that has been produced.

AB3 The agents know if they accept some proof-of-work.

AB4 An agent accepts at most one proof-of-work for a given round.

AB5 If a accepts c's proof of work for round j and (in the next step) b accepts a's proof-of-work for a later round, then b must also accept c's proof-of-work for round j. This essentially means that if b accepts a's proof-of-work, then b accepts the whole history of a.

AB6 If proofs-of-work for some round are produced, then each active agent must accept one of them. Note that we do not have any assumption on how an agent accepts a proof.

AB7 Only active agents can accept proofs-of-work.

AB8 If an agent accepts some proof-of-work for round $i+1$, then the agent also accepts some proof-of-work for round i.

AB9 If an agent accepts some proof-of-work for round i, then in the next round a proof-of-work for round $i+1$ must be available.

AB10 Only an agent that has accepted a proof-of-work for round i can create (in the next step) a proof-of-work for round $i+1$. This models the fact that a proof-of-work depends on the previously accepted history.

AB11 This says that possible forks are resolved at least after z rounds. Note that we do not have any assumption on how this consensus is achieved. This formalizes the *common prefix* property from [10].

Let us now briefly discuss the relationship between time instants (from the linear time logic part) and rounds (referenced in the atomic propositions in **POW** and **ACC**).

We start at time instant t and assume that agent b accepts some proof of work for round i, that means agent b accepts a blockchain of length i. Because of [AB9], at time instant $t+1$ some agent a will produce a proof-of-work for round $i+1$. By [AB1] at least one agent, say agent c, will be active at time instant $t+1$. By [AB6] agent c at time instant $t+1$ accepts some proof of work for round $i+1$, that means a blockchain of length $i+1$. Hence with every time instant, the accepted blockchain grows by one block.

However, we do not require that all proof-of-work for round $i+1$ is generated at time instant $t+1$. It is possible that some proof-of-work for round $i+1$ is produced at a later time instant.

Lemma 1. *The set of Blockchain Axioms is satisfiable.*

Proof. Construction of the model. Let $\mathbf{A} = \{a\}$, $R = \{r\}$, $\mathcal{K}_a(r_i) = \{r_i\}$, $a \in \mathcal{A}(r_i)$, for $i \geq 0$, $\mathsf{z} = 1$ and

- $r_i \models \mathsf{pow}_{a,i-k}$ iff $0 \leqslant k \leqslant i$,

- $r_i \models \mathsf{acc}_{a,a,i-k}$ iff $0 \leqslant k \leqslant i$,
- $r_i \models \neg\mathsf{acc}_{a,a,i'}$ iff $i \leqslant i'$.

This model satisfies the Blockchain axioms. □

A trivial consequence of [AB4] is that there cannot be an agreement of acceptance of two different proofs-of-work.

Lemma 2. *We have $e_{a,i} \to \neg e_{b,i}$ for $b \neq a$.*

Now we show that the common history persists, i.e., agreements cannot be undone.

Lemma 3. *We have $e_{a,i} \to \bigcirc e_{a,i}$.*

Proof. Assume $e_{a,i}$. We first show for any agents b and c that

$$\bigcirc\, \mathsf{acc}_{b,c,i+1} \to \mathsf{acc}_{c,a,i}. \tag{1}$$

Assume $\bigcirc\mathsf{acc}_{b,c,i+1}$. By [AB2] we get $\bigcirc\mathsf{pow}_{c,i+1}$. By [AB10] we obtain $\mathsf{ech}_{c,i}$. Since we assume $e_{a,i}$, this yields $\mathsf{acc}_{c,a,i}$ by [AB7]. Hence (1) is established.

Next we show for any agent b

$$\bigvee_c \bigcirc\mathsf{acc}_{b,c,i+1} \to \bigcirc\mathsf{acc}_{b,a,i}. \tag{2}$$

Because of (1) we find that $\bigvee_c \bigcirc\mathsf{acc}_{b,c,i+1}$ implies

$$\bigvee_c (\mathsf{acc}_{c,a,i} \wedge \bigcirc\mathsf{acc}_{b,c,i+1})$$

From [AB5] we have

$$\bigvee_c (\mathsf{acc}_{c,a,i} \wedge \bigcirc\mathsf{acc}_{b,c,i+1}) \to \bigcirc\mathsf{acc}_{b,a,i}$$

Thus we conclude $\bigcirc\mathsf{acc}_{b,a,i}$ and (2) is established

From $e_{a,i}$ and [AB1] we get $\bigvee_b \mathsf{acc}_{b,a,i}$. Then [AB9] yields $\bigcirc \bigvee_c \mathsf{pow}_{c,i+1}$. Thus from [AB6] we get

$$\bigwedge_b (\bigcirc A_b \to \bigcirc\mathsf{ech}_{b,i+1}).$$

Observe that $\bigcirc\mathsf{ech}_{b,i+1}$ is equivalent to $\bigvee_c \bigcirc\mathsf{acc}_{b,c,i+1}$. Hence by (2) we find

$$\bigwedge_b (\bigcirc A_b \to \bigcirc\mathsf{acc}_{b,a,i}),$$

which is equivalent to $\bigcirc e_{a,i}$. □

The next lemma says that if any of the agents has a choice in a round, then each active agent has its own choice in the same round.

Lemma 4. *We have* $A_b \wedge \mathsf{ech}_{a,i} \rightarrow \mathsf{ech}_{b,i}$.

Proof. From $\mathsf{ech}_{a,i}$ we obtain by [AB2] that $\bigvee_c \mathsf{pow}_{c,i}$. This together with A_b implies by [AB6] that $\mathsf{ech}_{b,i}$ holds. □

Theorem 6 states sufficient conditions that guarantee that common knowledge can be obtained.

Theorem 6. *We have*

$$\mathsf{ech}_{a,i+\mathsf{z}} \wedge \mathsf{acc}_{a,b,i} \rightarrow \mathtt{C}e_{b,i}$$

Proof. Let c be an arbitrary agent. Using [AB3] we find

$$\mathsf{ech}_{c,i+\mathsf{z}} \rightarrow \mathtt{K}_c\mathsf{ech}_{c,i+\mathsf{z}}$$

and

$$\mathsf{acc}_{c,b,i} \rightarrow \mathtt{K}_c\mathsf{acc}_{c,b,i}.$$

Hence by the $\mathtt{E}$ closure of [AB11] we find

$$\mathsf{ech}_{c,i+\mathsf{z}} \wedge \mathsf{acc}_{c,b,i} \rightarrow \mathtt{K}_c e_{b,i}.$$

Using Lemma 4 we get

$$A_c \wedge \mathsf{ech}_{a,i+\mathsf{z}} \wedge \mathsf{acc}_{c,b,i} \rightarrow \mathtt{K}_c e_{b,i}.$$

We have that $A_c \wedge e_{b,s} \rightarrow \mathsf{acc}_{c,b,s}$. Thus we obtain

$$A_c \wedge \mathsf{ech}_{a,i+\mathsf{z}} \wedge e_{b,i} \rightarrow \mathtt{K}_c e_{b,i}.$$

We have that $\neg A_c \rightarrow \mathtt{K}_c\bot$. Hence we have

$$\mathsf{ech}_{a,i+\mathsf{z}} \wedge e_{b,i} \rightarrow \mathtt{K}_c e_{b,i}.$$

Since c was arbitrary, this gives us

$$\mathsf{ech}_{a,i+\mathsf{z}} \wedge e_{b,i} \rightarrow \mathtt{E}e_{b,i}.$$

We even have

$$\mathtt{E}^k(\mathsf{ech}_{a,i+\mathsf{z}} \wedge e_{b,i} \rightarrow \mathtt{E}e_{b,i})$$

for all $k \in \mathbb{N}$ since all our assumptions are $\mathtt{E}$-closed. Thus we obtain

$$\mathsf{ech}_{a,i+\mathsf{z}} \wedge e_{b,i} \rightarrow \mathtt{E}^k e_{b,i}$$

for all $k \in \mathbb{N}$. Using [AB11] and [RIC] we finally conclude

$$\mathsf{ech}_{a,i+\mathsf{z}} \wedge \mathsf{acc}_{a,b,i} \rightarrow \mathtt{C}e_{b,i}.$$ □

As a corollary we get the following result.

Corollary 1. *The active agents have unique common history up to the last* z *rounds:*

$$\mathsf{ech}_{a,i+\mathsf{z}} \to \bigwedge_{k=0}^{i} (\mathsf{acc}_{a,b,k} \to \mathtt{C} e_{b,k}).$$

Proof. Let $0 \leq k \leq i$. From $\mathsf{ech}_{a,i+\mathsf{z}}$ we find by [AB8] that $\mathsf{ech}_{a,k+\mathsf{z}}$. By Theorem 6 we find

$$\mathsf{acc}_{a,b,k} \to \mathtt{C} e_{b,k},$$

which yields the desired result. □

This property can be compared with the *persistence* property of [10]—a transaction that goes more than k blocks "deep" into the blockchain of one honest player will be included in every honest player's blockchain with overwhelming probability, and it will be assigned a permanent position in the ledger. So, Theorem 1 corresponds to [10, Theorem 15], [18, Theorem 5.2] and [34, Claim 6.2]. In our opinion, beside differences related to our proof-theoretic approach and the approach from [18] which is model-theoretic, the assumptions about the protocol formalized by the above given axioms are somehow more primitive than the ones given in [18]. That is why we can express, for example, how ledgers are changed in each round and how acceptance (by an agent) of a proof-of-work produced by another agent affects the ledger of the former agent, while [18] mostly discuss how a consensus between all agents can be achieved.

[AB11] states that forks will be resolved after a fixed number of rounds. Another possibility how forks can be resolved is when in a round only one proof-of-work is available. In that case, everyone has to accept the unique proof-of-work, i.e., everyone agrees on it.

Lemma 5. *The following is common knowledge:* $\mathsf{pow}_{b,i} \wedge \bigwedge_{c \neq b} \neg \mathsf{pow}_{c,i} \to e_{b,i}$.

Proof. Suppose towards a contradiction that $\neg \mathsf{acc}_{a,b,s}$ for some a with A_a. From $\mathsf{pow}_{b,i}$ and A_a we get by [AB6] that $\mathsf{ech}_{a,i}$. Because of $\neg \mathsf{acc}_{a,b,s}$ we have $\bigvee_{d \neq b} \mathsf{acc}_{a,d,i}$. Hence by [AB2] we conclude $\bigvee_{d \neq b} \mathsf{pow}_{d,i}$, which contradicts the assumption $\bigwedge_{c \neq b} \neg \mathsf{pow}_{c,i}$. Thus

$$\mathsf{pow}_{b,i} \wedge \bigwedge_{c \neq b} \neg \mathsf{pow}_{c,i} \to e_{b,i} \tag{3}$$

is established. Since our theory includes the $\mathtt{E}$-closure of [AB6] and [AB2], we also have the $\mathtt{E}$-closure of (3) and by [RIC] finally also common knowledge of (3). □

In Theorem 6 we showed that after a fixed number of rounds, we not only have an agreement, but also that this agreement is common knowledge. In the case of the previous lemma, we also get an agreement, but there, the agreement is not common knowledge. To obtain common knowledge of a unique proof-of-work, we need an additional assumption about the blockchain protocol.

AB12 $\neg \mathsf{pow}_{a,i} \to \mathtt{E}\neg \mathsf{pow}_{a,i}$

[AB12] states that if agent a does not produce a proof-of-work in the round i, then everybody knows that. From [AB1]–[AB11] it follows that in each round each agent receives *at least one* of the generated proofs-of-work. [AB12] requires that each agent receives *all* generated proofs-of-work. Note that this means that all messages will not be delayed or lost, which is a stronger assumption than the one used so far ("while some messages may get lost, in every round every active agent receives at least one new block"). Under this additional assumption, we can show that a unique proof-of-work leads to common knowledge. This property can be compared to *liveness* property in [10]: every transaction is eventually executed and every participant includes it in their own ledger.

Theorem 7. *Assume our blockchain theory also includes (the* $\mathtt{E}$*-closure of) [AB12]. Then we have* $\mathsf{pow}_{b,i} \wedge \bigwedge_{c \neq b} \neg \mathsf{pow}_{c,i} \to \mathtt{C} e_{b,i}$.

Proof. We first show

$$\mathsf{pow}_{b,i} \wedge \bigwedge_{c \neq b} \neg \mathsf{pow}_{c,i} \to \mathtt{E}\mathsf{pow}_{b,i} \wedge \mathtt{E} e_{b,i}. \tag{4}$$

Assume $\mathsf{pow}_{b,i} \wedge \bigwedge_{c \neq b} \neg \mathsf{pow}_{c,i}$. By Lemma 5 we get $e_{b,i}$. For any a with A_a we get $\mathsf{acc}_{a,b,i}$ and by [AB3] also $\mathtt{K}_a \mathsf{acc}_{a,b,i}$. Thus, by [AB2] $\mathtt{K}_a \mathsf{pow}_{b,i}$. Since a was arbitrary (and by $\neg A_a \implies \mathtt{K}_a \bot$), we get $\mathtt{E}\, \mathsf{pow}_{b,i}$. Further [AB12] yields $\bigwedge_{c \neq b} \mathtt{E} \neg \mathsf{pow}_{c,i}$. Thus by Lemma 5 we find $\mathtt{E} e_{b,i}$ and (4) is established.

Since our theory includes the $\mathtt{E}$-closure of [AB2], [AB3], and [AB12], we not only have (4) but also its $\mathtt{E}$-closure, i.e.

$$\mathtt{E}^k(\mathsf{pow}_{b,i} \wedge \bigwedge_{c \neq b} \neg \mathsf{pow}_{c,i} \to \mathtt{E}\mathsf{pow}_{b,i} \wedge \mathtt{E} e_{b,i}) \quad \text{for all } k \in \mathbb{N}. \tag{5}$$

Now observe that by the the $\mathtt{E}$-closure of [AB12]

$$\neg \mathsf{pow}_{a,i} \to \mathtt{E}^k \neg \mathsf{pow}_{a,i} \quad \text{for all } k \in \mathbb{N}.$$

Therefore, using (5) we find

$$\mathsf{pow}_{b,i} \wedge \bigwedge_{c \neq b} \neg \mathsf{pow}_{c,i} \to \mathtt{E}^k e_{b,i} \quad \text{for all } k \in \mathbb{N}.$$

By [RIC], we finally conclude

$$\mathsf{pow}_{b,i} \wedge \bigwedge_{c \neq b} \neg \mathsf{pow}_{c,i} \to \mathtt{C} e_{b,i}. \qquad \square$$

4 Conclusion

In this paper, we provide a strongly complete axiomatization of three related temporal epistemic logics which differ in the approach to the ability of agents to

join or leave the system. We employ this framework for an axiomatic approach to study the blockchain protocol in a synchronous setting in which agents are allowed to enter/leave the network. We investigate which assumptions about a blockchain protocol entail which properties of the protocol. In particular, we show how blockchains can be used to achieve common knowledge among a set of agents.

In this paper we use the notion "proof-of-work" to denote production of a solution of a problem related to a set of transactions, without considering what a transaction represents (it can be a transfer of bitcoins, or a smart contract, etc.), or what is the procedure to obtain a solution (it can be proof-of-work used for bitcoins, but also proof-of-memory, proof-of-authority, proof-of-stake, etc.). Also, we do not assume any specific way to achieve consensus between agents (it can be acceptance of fastest solution, Byzantine agreement, etc.).

We plan to extend our formal framework to support a more general modeling of blockchains. One of possible directions is to add probability operators to the formal language, so that we can express statements like: "Older transactions have a higher probability of not being reversed". Another challenge will be to use our approach in automated reasoning about the blockchain protocol (using proof assistants like, e.g., Coq or Isabelle/HOL).

Funding

This work was supported by Serbian Ministry of Education, Science and Technology Development through Matematički institut SANU [ON174026, III44006 to B.M. and Z.O.]; and Ministarstvo znanosti, obrazovanja i športa republike Hrvatske [to P.G.], and the Swiss National Science Foundation [200021_165549 to T.S.].

Acknowledgements

Thomas Studer would like to thank Kai Brünnler, Hans van Ditmarsch, Dandolo Flumini, and Ioannis Kokkinis for many inspiring discussions about blockchain protocols and their logical modeling.

The authors thank the anonymous referees whose comments helped clarify a number of points and improve the text.

References

[1] M. Abadi, J.Y. Halpern. *Decidability and expressiveness for first-order logics of probability.* Information and Computation 112(1) 1–36, 1994.

[2] P. Balbiani, D. Vakarelov. *Iteration-free PDL with Intersection: a Complete Axiomatization.* Fundamenta Informaticae 45(3), 173–194, 2001.

[3] K. Brünnler. *Deep sequent systems for modal logic*. In G. Governatori, I. Hodkinson, and Y. Venema, editors, *Advances in Modal Logic*, volume 6, pages 107–119. College Publications, 2006.

[4] K. Brünnler. *Blockchain kurz & gut*. O'Reilly, 2018.

[5] K. Brünnler, D. Flumini, T. Studer. *A Logic of Blockchain Updates*. In S. Artemov and A. Nerode, editors, *Logical Foundations of Computer Science LFCS 18*, volume 10703 of *LNCS*, pages 107–119. Springer, 2018.

[6] K. Brünnler, T. Studer. *Syntactic cut-elimination for common knowledge*. Annals of Pure and Applied Logic 160 (1), 82–95, 2009.

[7] K. Brünnler, T. Studer. *Syntactic cut-elimination for a fragment of the modal mu-calculus*. Annals of Pure and Applied Logic 163 (12), 1838–1853, 2012.

[8] J.P. Burgess. *Axioms for tense logic. I. Since and until*. Notre Dame Jourbnal of Formal Logic 23(4), 367–374 1982.

[9] C. Decker, R. Wattenhofer. *Information propagation in the Bitcoin network*. In 13th IEEE International Conference on Peer-to-Peer Computing, pages 1–10. 2013

[10] J. Garay, A. Kiayias, N. Leonardos. *The Bitcoin Backbone Protocol: Analysis and Applications*. Cryptology ePrint Archive, https://eprint.iacr.org/2014/765.pdf, 2017.

[11] R. Goldblatt. *Axiomatising the Logic of Computer Programming*. Lecture Notes in Computer Science 130. Springer-Verlag, 1982.

[12] R. Goldblatt. *Logics of Time and Computation*. Center for the Study of Language and Information, Second Edition, 1992.

[13] A. Grove, J. Halpern. *Naming and identity in epistemic logics, I: The propositional case*. Journal of Logic and Computation, 3:4, 345–378, 1993.

[14] C. Grunspan, R. Pérez-Marco. *Double spend races*. ArXiv e-prints 1702.02867. 2017

[15] R. Fagin, J. Halpern, Y. Moses, M. Y. Vardi. *Reasoning About Knowledge*. The MIT Press, Cambridge, Massachusetts, 1995.

[16] J. Halpern, R. Fagin. *Modelling knowledge and action in distributed systems*. Distributed Computing 3, 159–177, 1989.

[17] J. Halpern, Y. Moses. *Knowledge and common knowledge in a distributed environment*. Journal of the ACM 37:3, 549–587, 1990.

[18] J. Halpern, R. Pass. *A Knowledge-Based Analysis of the Blockchain Protocol*. In J. Lang, edt., Proceedings of the Sixteenth Conference on Theoretical Aspects of Rationality and Knowledge, TARK 2017, Liverpool, UK, 24–26 July 2017. Electronic Proceedings in Theoretical Computer Science 251, 324–335, 2017. `https://arxiv.org/pdf/1707.08751v1.pdf`

[19] J. Halpern, R. van der Meyden and M. Vardi. *Complete axiomatizations for reasoning about knowledge and time*. SIAM Journal on Computing 33:2, 674–703, 2004.

[20] J. Hintikka. *Knowledge and Belief: An Introduction to the Logic of the Two Notions*. Cornell University Press, 1962.

[21] G. Jäger, M. Kretz, and T. Studer. Cut-free common knowledge. *Journal Applied Logic*, 5(4):681–689, 2007.

[22] H. Kamp. *Tense Logic and the Theory of Linear Order*. Doctoral disertation, University of California at Los Angeles, 1968.

[23] S. Kraus, D. Lehmann. *Knowledge, belief and time*. Theoretical Computer Science 58, 155–174, 1988.

[24] O. Lichtenstein and A. Pnueli. *Propositional temporal logics: Decidability and completeness*. Logic Journal of the IGPL, 8(1):55–85, 2000.

[25] Z. Manna and A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems: Specification*. Springer-Verlag, 1992.

[26] B. Marinković, Z. Ognjanović, D. Doder, A. Perović. *A Propositional Linear Time logic with Time Flow Isomorphic to* ω^2. Journal of Applied Logic, 12(2), 208–229, 2014.

[27] M. Marti, T. Studer. *The Proof Theory of Common Knowledge*. In H. van Ditmarsch and G. Sandu, edts., Jaakko Hintikka on knowledge and game theoretical semantics, 433–455, Springer, 2017.

[28] J.-J. Meyer and W. van der Hoek. *Epistemic Logic for AI and Computer Science*. Cambridge University Press, 1995.

[29] M. Milošević, Z. Ognjanović. *A First-Order Conditional Probability Logic With Iterations*. Publication de L'Institute Matematique, n.s. 93 (107), 19–27, 2013.

[30] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. `https://bitcoin.org/bitcoin.pdf`. 2009.

[31] Z. Ognjanović. *Discrete Linear-time Probabilistic Logics: Completeness, Decidability and Complexity*. Journal of Logic Computation, Vol. 16, No. 2, 257–285, 2006.

[32] Z. Ognjanović, D. Doder, Z. Marković. *A Branching Time Logic with Two Types of Probability Operators.* Fifth International Conference on Scalable Uncertainty Management SUM-2011, Springer LNCS 6929, 219–232, 2011.

[33] Z. Ognjanović, M. Rašković, Z. Marković. *Probability Logics: Probability-Based Formalization of Uncertain Reasoning.* Springer, 2016.

[34] R. Pass, L. Seeman, A. Shelat. *Analysis of the Blockchain Protocol in Asynchronous Networks.* Cryptology ePrint Archive, https://eprint.iacr.org/2016/454.pdf , 2016.

[35] A. N. Prior. *Time and Modality.* Clarendon Press, Oxford, 1957.

[36] K. Segerberg. *A model existence theorem in infinitary propositional modal logic.* Journal of Philosophical Logic, Volume 23, Issue 4, 337–367, 1994.

[37] G. Sundholm *A completeness proof for an infinitary tense-logic.* Theoria 43, 47–51., 1977.

[38] A. Szalas, L. Holenderski. Incompleteness of first-order temporal logic with until. *Theoretical Computer Science*, 73(1), 317–325, 1988.

[39] S. Tomović, Z. Ognjanović, D. Doder. *Probabilistic Common Knowledge Among Infinite Number of Agents.* Proceedings of the ECSQARU 2015, LNCS 9161, 496–505, 2015.

A Proofs

Theorem 1. *[Soundness for* $\mathtt{Ax}_{nr}$*]* $\vdash_{nr} \beta$ *implies* $\models_{nr} \beta$.

Proof. Validity of the axioms and rules [MP], [RTN] and [RKN] can be proved in a standard way (see [26, 31, 32]).

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

We will show by induction that [RIU] produces valid formulas from valid sets of premises.

Suppose that

$$r_s\models\Phi_k(\bigcirc^m\neg((\bigwedge_{l=0}^{i-1}\bigcirc^l\beta_1)\wedge\bigcirc^i\beta_2),(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}}),\text{ for } i\geqslant 0.$$

Induction base. Let $k=0$.

If $r_s\not\models\theta_0\rightarrow\bigcirc^m\neg(\beta_1\mathtt{U}\beta_2)$ then

$r_s\models\theta_0\wedge\bigcirc^m(\beta_1\mathtt{U}\beta_2)$ iff

$r_s\models\theta_0$ and $r_s\models\bigcirc^m(\beta_1\mathtt{U}\beta_2)$ iff

$r_s \models \theta_0,\ r_{s+m+i_0} \models \beta_2,\ \text{and } r_{s+m+l} \models \beta_1,\ \text{for some } i_0 \geqslant 0,\ \text{and } 0 \leqslant l < i_0$ (6)

On the other hand, $r_s \models \theta_0 \rightarrow \bigcirc^m \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2)$ for all $i \geqslant 0$ iff for all $i \geqslant 0$

$$r_s \models \neg\theta_0 \text{ or } r_{s+m+i} \not\models \beta_2 \text{ or } r_{s+m+l} \not\models \beta_1,\ 0 \leqslant l < i \tag{7}$$

which contradicts (6).

Inductive step. Let

$$r_s \models \Phi_{k+1}(\bigcirc^m \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$$

for all $i \geqslant 0$, i.e.,

$$r_s \models \theta_{k+1} \rightarrow \mathtt{B}_k\Phi_k(\bigcirc^m \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}}) \tag{8}$$

for all $i \geqslant 0$.

Let us assume the opposite:

$$r_s \not\models \Phi_{k+1}(\bigcirc^m \neg(\beta_1 \mathtt{U} \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}}),\ \text{i.e.,}$$

$$r_s \models \theta_{k+1} \wedge \neg\mathtt{B}_k\Phi_k(\bigcirc^m \neg(\beta_1 \mathtt{U} \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}}). \tag{9}$$

From (8) and (9) we have:

$$r_s \models \mathtt{B}_k\Phi_k(\bigcirc^m \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$$

for all $i \geqslant 0$, and

$$r_s \not\models \mathtt{B}_k\Phi_k(\bigcirc^m \neg(\beta_1 \mathtt{U} \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}}).$$

Assume now that $\mathtt{B}_k$ is empty. Then, by the induction hypothesis from

$$r_s \models \Phi_k(\bigcirc^m \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$$

for all $i \geqslant 0$, we infer

$$r_s \models \Phi_k(\bigcirc^m \neg(\beta_1 \mathtt{U} \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}}).$$

Next, assume that $\mathtt{B}_k = \bigcirc\mathtt{B'}_k$ and that the statement can be proved for $\mathtt{B'}_k$. Then we have:

$r_s \models \bigcirc \mathtt{B}'_k \Phi_k(\bigcirc^m \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$, for all $i \geqslant 0$, iff

$r_{s+1} \models \mathtt{B}'_k \Phi_k(\bigcirc^m \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$, for all $i \geqslant 0$, iff

by I.H. $r_{s+1} \models \mathtt{B}'_k \Phi_k(\bigcirc^m \neg(\beta_1 \mathtt{U} \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$ iff

$r_s \models \bigcirc \mathtt{B}'_k \Phi_k(\bigcirc^m \neg(\beta_1 \mathtt{U} \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$.

Finally, let $\mathtt{B}_k = \mathtt{K}_e \mathtt{B}'_k$. Then, for every $r_{s'}^{j'} \in \mathcal{K}_e(r_s)$ we have that:

$$r_{s'}^{j'} \models \mathtt{B}'_k \Phi_k(\bigcirc^m \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$$

for all $i \geqslant 0$, and by the induction hypothesis

$$r_{s'}^{j'} \models \mathtt{B}'_k \Phi_k(\bigcirc^m \neg(\beta_1 \mathtt{U} \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}}).$$

Therefore:

$$r_s \models \mathtt{K}_e \mathtt{B}'_k \Phi_k(\bigcirc^m \neg(\beta_1 \mathtt{U} \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$$

which is a contradiction.

RIC can be proved similarly.

□

Theorem 8 (Deduction theorem)**.** *$T \cup \{\varphi\} \vdash \psi$ implies $T \vdash \varphi \to \psi$.*

Proof. If ψ is an axiom or $\psi \in T$, then $T \vdash \psi$, so since $T \vdash \psi \to (\varphi \to \psi)$ (Axiom [A]), by [MP] $T \vdash \varphi \to \psi$. If $\varphi = \psi$ then $T \vdash \varphi \to \varphi$ by Axiom [A].

If ψ is a theorem then, $\vdash \bigcirc\psi$. By weakening $T \vdash \bigcirc\psi$, so $T \vdash \varphi \to \bigcirc\psi$. Similarly for [RKN] rule.

Let us assume that ψ is obtained from $T \cup \{\varphi\}$ using [RIU] rule, i.e. $\psi = \Phi_k(\neg(\beta_1 \mathtt{U} \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$. Then we have:

$T, \varphi \vdash \Phi_k(\bigcirc^m \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$ for all $i \geqslant 0$,

$T \vdash \varphi \to \Phi_k(\bigcirc^m \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$, by induction hypothesis,

$T \vdash \varphi \to (\theta_k \to \mathtt{B}_{k-1} \Phi_{k-1}(\bigcirc^m \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}}))$, by the definition of Φ_k

$T \vdash (\varphi \wedge \theta_k) \to \mathtt{B}_{k-1} \Phi_{k-1}(\bigcirc^m \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$, by propositional tautology $(p \to (q \to r)) \leftrightarrow ((p \wedge q) \to r)$.

If $(\bar{\theta}_j)_{j\in\mathbb{N}}$ denotes the sequence which coincides everywhere with $(\theta_j)_{j\in\mathbb{N}}$ for $j \neq k$, with the exception that $\bar{\theta}_k \equiv \varphi \wedge \theta_k$ we get that:

$T \vdash \bar{\theta}_k \to \mathtt{B}_{k-1}\Phi_{k-1}(\bigcirc^m\neg((\bigwedge_{l=0}^{i-1}\bigcirc^l\beta_1)\wedge\bigcirc^i\beta_2),(\bar{\theta}_j)_{j\in\mathbb{N}})$,

$T \vdash \Phi_k(\bigcirc^m\neg((\bigwedge_{l=0}^{i-1}\bigcirc^l\beta_1)\wedge\bigcirc^i\beta_2),(\bar{\theta}_j)_{j\in\mathbb{N}})$ for all $i \geqslant 0$,

$T \vdash \Phi_k(\bigcirc^m\neg(\beta_1\mathtt{U}\beta_2),(\bar{\theta}_j)_{j\in\mathbb{N}})$ by [RIU]

$T \vdash (\varphi\wedge\theta_k) \to \mathtt{B}_{k-1}\Phi_{k-1}(\bigcirc^m\neg(\beta_1\mathtt{U}\beta_2),(\bar{\theta}_j)_{j\in\mathbb{N}})$

$T \vdash \varphi \to (\theta_k \to \mathtt{B}_{k-1}\Phi_{k-1}(\bigcirc^m\neg(\beta_1\mathtt{U}\beta_2),(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}}))$

$T \vdash \varphi \to \Phi_k(\bigcirc^m\neg(\beta_1\mathtt{U}\beta_2),(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}}))$

$T \vdash \varphi \to \psi$.

The same holds for [RIC].

□

Definition 7. *For a given set of formulas T,*

$$*T = \{*\alpha | \alpha \in T\}, \qquad *^{-1}(T) = \{\alpha | * \alpha \in T\}$$

for $* \in \{\mathtt{K}_a, \mathtt{C}, \bigcirc, \}$. □

For example, $\mathtt{K}_a^{-1}(T) = \{\alpha | \mathtt{K}_a\alpha \in T\}$.

Lemma 6. *Let α, β be formulas:*

LF1 $\vdash \mathtt{G}\beta \leftrightarrow \beta\wedge\bigcirc\mathtt{G}\beta$,

LF2 $\vdash \mathtt{G}\bigcirc\beta \leftrightarrow \bigcirc\mathtt{G}\beta$,

LF3 $(\bigcirc\beta_1 \to \bigcirc\beta_2) \to \bigcirc(\beta_1 \to \beta_2)$,

LF4 $(\bigcirc\beta_1 \wedge \bigcirc\beta_2) \leftrightarrow \bigcirc(\beta_1 \wedge \beta_2)$,

LF5 $(\bigcirc\beta_1 \vee \bigcirc\beta_2) \leftrightarrow \bigcirc(\beta_1 \vee \beta_2)$,

LF6 $\mathtt{G}\beta \vdash \bigcirc^i\beta$, $i \geqslant 0$,

LF7 if $\vdash \beta$ *then* $\vdash \mathtt{G}\beta$,

LF8 if $T \vdash \beta$, *where T is a set of formulas, then* $\bigcirc T \vdash \bigcirc\beta$,

LF9 for $j \geqslant 0$, $\bigcirc^j\beta_2, \bigcirc^0\beta_1, \ldots, \bigcirc^{j-1}\beta_1 \vdash \beta_1\mathtt{U}\beta_2$,

LK if $T \vdash \gamma$, *where T is a set of formulas, then* $\mathtt{K}_eT \vdash \mathtt{K}_e\gamma$.

Proof. LF1 $\vdash \mathtt{G}\beta \leftrightarrow \beta\wedge\bigcirc\mathtt{G}\beta$

$\vdash \neg(\top\mathtt{U}\neg\beta) \leftrightarrow \neg(\neg\beta\vee(\top\wedge\bigcirc(\top\mathtt{U}\neg\beta)))$ (by definition of $\mathtt{G}$ and [AT3])

$\vdash \neg(\top\mathtt{U}\neg\beta) \leftrightarrow \beta\wedge(\bot\vee\bigcirc\neg(\top\mathtt{U}\neg\beta))$ (by [AT1])

$\vdash \neg(\top\mathtt{U}\neg\beta) \leftrightarrow \beta\wedge\bigcirc\neg(\top\mathtt{U}\neg\beta)$ (property of $\vee$)

$\vdash \mathtt{G}\beta \leftrightarrow \beta\wedge\bigcirc\mathtt{G}\beta$ (by definition of $\mathtt{G}$)

LF2–LF7 The proofs are the consequences of the temporal part of the above axiomatization.

LF8 if $T \vdash \beta$, where T is a set of formulas, then $\bigcirc T \vdash \bigcirc\beta$

We will prove this by the induction on the length of the proof of β from T. Suppose that β is obtained by the inference rule [MP] from $\beta_2 \to \beta_1$ and β_2. Then we have:

$\bigcirc T \vdash \bigcirc(\beta_2 \to \beta_1)$ (induction hypothesis)

$\bigcirc T \vdash \bigcirc(\beta_2 \to \beta_1) \to (\bigcirc\beta_2 \to \bigcirc\beta_1)$ [AT2]

$\bigcirc T \vdash \bigcirc\beta_2 \to \bigcirc\beta_1$ [MP]

$\bigcirc T \vdash \bigcirc\beta_2$ (induction hypothesis)

$\bigcirc T \vdash \bigcirc\beta_1$ [MP]

Similarly we can prove the cases when β is obtained using [RTN] and [RKN]. Suppose that

$$\begin{aligned}\beta &= \Phi_k(\bigcirc^s\neg(\beta_1\mathtt{U}\beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})\\ &= \theta_k \to \mathtt{B}_{k-1}\Phi_{k-1}(\bigcirc^s\neg(\beta_1\mathtt{U}\beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})\end{aligned}$$

is obtained by the inference rule [RIU]. Recall that $\mathtt{B}_k$ is a sequence of alternating blocks of the operators $\bigcirc$ and $\mathtt{K}_a$. Then:

$\bigcirc T \vdash \bigcirc\Phi_k(\bigcirc^s\neg((\bigwedge_{l=0}^{i-1}\bigcirc^l\beta_1) \wedge \bigcirc^i\beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$, for $i \geqslant 0$, by the induction hypothesis

$\bigcirc T \vdash \bigcirc(\theta_k \to \mathtt{B}_{k-1}\Phi_{k-1}(\bigcirc^s\neg((\bigwedge_{l=0}^{i-1}\bigcirc^l\beta_1)\wedge\bigcirc^i\beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}}))$, for $i \geqslant 0$

$\bigcirc T \vdash \bigcirc\Big(\theta_k \to \mathtt{B}_{k-1}\Phi_{k-1}(\bigcirc^s\neg((\bigwedge_{l=0}^{i-1}\bigcirc^l\beta_1) \wedge \bigcirc^i\beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})\Big) \to \Big(\bigcirc\theta_k \to \bigcirc\mathtt{B}_{k-1}\Phi_{k-1}(\bigcirc^s\neg((\bigwedge_{l=0}^{i-1}\bigcirc^l\beta_1) \wedge \bigcirc^i\beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})\Big)$, for $i \geqslant 0$, by [AT2]

$\bigcirc T \vdash \bigcirc\theta_k \to \bigcirc\mathtt{B}_{k-1}\Phi_{k-1}(\bigcirc^s\neg((\bigwedge_{l=0}^{i-1}\bigcirc^l\beta_1)\wedge\bigcirc^i\beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$, for $i \geqslant 0$, by [MP]

$\bigcirc T \vdash (\bigcirc\theta_k \to \bigcirc\mathtt{B}_{k-1}\Phi_{k-1}(\bigcirc^s\neg(\beta_1\mathtt{U}\beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}}))$, by [RIU]

$\bigcirc T \vdash (\bigcirc\theta_k \to \bigcirc\mathtt{B}_{k-1}\Phi_{k-1}(\bigcirc^s\neg(\beta_1\mathtt{U}\beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})) \to (\bigcirc(\theta_k \to \mathtt{B}_{k-1}\Phi_{k-1}(\bigcirc^s\neg(\beta_1\mathtt{U}\beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})))$, by (LF3)

$\bigcirc T \vdash \bigcirc(\theta_k \to \mathtt{B}_{k-1}\Phi_{k-1}(\bigcirc^s\neg(\beta_1\mathtt{U}\beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}}))$, by [MP]

$\bigcirc T \vdash \bigcirc\Phi_k(\bigcirc^s\neg(\beta_1\mathtt{U}\beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$.

The proof which concerns the rule [RIC] is similar.

LF9 for $j \geqslant 0$, $\bigcirc^j\beta_2, \bigcirc^0\beta_1, \ldots, \bigcirc^{j-1}\beta_1 \vdash \beta_1 \mathtt{U} \beta_2$

By propositional reasoning we can obtain:

$$\begin{aligned}\bigcirc^j\beta_2, \bigcirc^0\beta_1, \ldots, \bigcirc^{j-1}\beta_1 \vdash & \beta_2 \vee (\beta_1 \wedge (\bigcirc\beta_2 \vee (\bigcirc\beta_1 \wedge (\ldots \\ & (\bigcirc^{j-1}\beta_2 \vee (\bigcirc^{j-1}\beta_1 \wedge (\bigcirc^j\beta_2 \vee \\ & (\bigcirc^j\beta_1 \wedge \bigcirc^{j+1}(\beta_1 \mathtt{U} \beta_2)))))) \ldots))).\end{aligned}$$

Since

$$\vdash \beta \vee (\alpha \wedge (\bigcirc\beta \vee (\bigcirc\alpha \wedge (\ldots (\bigcirc^{j-1}\beta \vee (\bigcirc^{j-1}\alpha \wedge (\bigcirc^j\beta \vee (\bigcirc^j\alpha \wedge \bigcirc^{j+1}(\alpha \mathtt{U} \beta)))))) \ldots))) \rightarrow \alpha \mathtt{U} \beta$$

can be gained using [AT3], we have

$$\bigcirc^j\beta_2, \bigcirc^0\beta_1, \ldots, \bigcirc^{j-1}\beta_1 \vdash \beta_1 \mathtt{U} \beta_2.$$

LK if $T \vdash \beta$, where T is a set of formulas, then $\mathtt{K}_e T \vdash \mathtt{K}_e \beta$.

We use the transfinite induction on the length of the proof $T \vdash \beta$. Suppose that $T \vdash \beta$ where $\beta \equiv \Phi_k(\bigcirc^s \neg(\beta_1 \mathtt{U} \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$ is obtained using [RIU].Then:

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

$\mathtt{K}_e T \vdash \mathtt{K}_e \Phi_k(\bigcirc^s \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$, for all $i \geq 0$, by the induction hypothesis

$\mathtt{K}_e T \vdash \top \rightarrow \mathtt{K}_e \Phi_k(\bigcirc^s \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2), (\theta_j)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})$, for all $i \geq 0$, by propositional reasoning

$\mathtt{K}_e T \vdash \Phi_{k+1}(\bigcirc^s \neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \beta_1) \wedge \bigcirc^i \beta_2), (\bar{\theta}_j)_{j\in\mathbb{N}})$, where $(\bar{\theta}_j)_{j\in\mathbb{N}}$ is a nested $k+1$-sequence such that $\bar{\theta}_{k+1} \equiv \top$, $\bar{\theta}_k \equiv \mathtt{K}_e\theta_k$, and otherwise coincides with $(\mathtt{K}_e\theta_j)_{j\in\mathbb{N}}$

$\mathtt{K}_e T \vdash \Phi_{k+1}(\bigcirc^s \neg(\beta_1 \mathtt{U} \beta_2), (\bar{\theta}_j)_{j\in\mathbb{N}}))$, by [RIU]

$\mathtt{K}_e T \vdash \top \rightarrow \mathtt{K}_e \Phi_k(\bigcirc^s \neg(\beta_1 \mathtt{U} \beta_2), (\bar{\theta}_j)_{j\in\mathbb{N}}))$

$\mathtt{K}_e T \vdash \mathtt{K}_e \beta$.

The case for the rule [RIC] is similar.

□

Theorem 2. *Every $\mathtt{Ax}_{nr}$-consistent set of formulas F can be extended to a maximal $\mathtt{Ax}_{nr}$-consistent set F^*.*

Proof. Let us assume that $For = \{\beta_i | i \geqslant 0\}$ is the set of all formulas. The maximally consistent set T^* is defined recursively, as follows:

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 $\Phi_k(\mathtt{C}\beta,(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}})$ 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. $T^*=\bigcup_{n\geqslant 0}T_n$.

The sets obtained by the steps 2 or 5 are obviously consistent. Let us consider the step 3. If

$$\neg\Phi_k(\bigcirc^s\neg((\bigwedge_{l=0}^{n-1}\bigcirc^l\beta^{'})\wedge\bigcirc^n\beta^{''}),(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}})$$

is not consistent with T_i for every $n\geqslant 0$ then by Deduction theorem,

$$T_i\vdash\Phi_k(\neg(\bigcirc^s(\bigwedge_{l=0}^{n-1}\bigcirc^l\beta^{'})\wedge\bigcirc^n\beta^{''}),(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}})$$

for every $n\geqslant 0$, and by [RIU] we have

$$T_i\vdash\Phi_k(\bigcirc^s\neg(\beta^{'}\mathtt{U}\beta^{''}),(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}}))$$

which contradicts the assumption. Thus, the set T_i obtained by the step 3 is also consistent. In a similar way we can prove that the step 4 produces consistent sets.

Since the construction guarantees that for each $\beta^{'}\in For$, either $\beta^{'}\in T^*$ or $\neg\beta^{'}\in T^*$, it follows that T^* is maximal. T^* does not contain all formulas because it is not possible that both β_i and $\beta_j=\neg\beta_i$ belong to $T_{1+\max\{i,j\}}$.

Finally, to prove that T^* is deductively closed, it is sufficient to prove that it is closed under the inference rules. We will only prove closeness under the inference rule [RIU], and the other cases follow similarly.

Suppose that

$$\Phi_k(\bigcirc^s\neg(\beta^{'}\mathtt{U}\beta^{''}),(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}}))\notin T^*$$

while

$$\Phi_k(\bigcirc^s\neg((\bigwedge_{l=0}^{n-1}\bigcirc^l\beta^{'})\wedge\bigcirc^n\beta^{''}),(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}})\in T^*$$

for every $n \geqslant 0$. By maximality of T^*,

$$\neg\Phi_k(\bigcirc^s\neg(\beta^{'}\mathtt{U}\beta^{''}),(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}}) \in T^*.$$

If $\beta_i = \Phi_k(\bigcirc^s\neg(\beta^{'}\mathtt{U}\beta^{''}),(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}}))$, then, by the construction of T^* there is i_0 such that

$$\neg\Phi_k(\bigcirc^s\neg((\bigwedge_{l=0}^{i_0-1}\bigcirc^l\beta^{'})\wedge\bigcirc^{i_0}\beta^{''}),(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}}) \in T_i$$

which contradicts the fact that

$$\Phi_k(\neg((\bigwedge_{l=0}^{n-1}\bigcirc^l\beta^{'})\wedge\bigcirc^n\beta^{''}),(\theta_j)_{j\in\mathbb{N}},(\mathtt{B}_j)_{j\in\mathbb{N}}) \in T^*$$

for every $n \geqslant 0$. □

Canonical structure.

Let $\mathcal{W}$ be the family of all maximal consistent sets. For every $W \in \mathcal{W}$ we consider the following sequence of sets of formulas $W_0 = W$, and $W_s = \{\beta : \bigcirc\beta \in W_{s-1}\}$, $s > 0$. We can prove that every set in that sequence is maximal and consistent.

Lemma 7. *Every W_s is a maximal consistent set.*

Proof. The proof is by induction on s. By the assumption every W_0 is maximal and consistent. Let $s \geqslant 0$ and W_s be maximal and consistent.

Suppose that W_{s+1} is not maximal. There is a formula β such that $\{\beta, \neg\beta\}\cap W_{s+1} = \varnothing$. Consequently, $\{\bigcirc\beta, \bigcirc\neg\beta\}\cap W_s = \varnothing$, which is in contradiction with maximality of W_s.

Suppose that W_{s+1} is not consistent, i.e., $W_{s+1} \vdash \beta \wedge \neg\beta$, for any formula β. By [LF8], $\bigcirc W_{s+1} \vdash \bigcirc(\beta \wedge \neg\beta)$ and $W_s \vdash \bigcirc(\beta \wedge \neg\beta)$. By [LF4] and [AT1] we can show that $W_s \vdash \bigcirc\beta \wedge \neg \bigcirc \beta$, which is in contradiction with consistency of W_s. □

Next, we define a special, so called canonical structure

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

such that:

- for every $W \in \mathcal{W}$, a run is the sequence $r^W = \langle W_0, W_1, \ldots\rangle$, where $W = W_0$, 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 $\mathtt{K}_a^{-1}(W_i) \subset W'_{i'}$.

Note that, if $a \notin \mathcal{A}(r_i^W)$, i.e., there is a formula β such that $K_a\beta \wedge K_a\neg\beta \in W_i$, then $\beta \wedge \neg\beta \in \mathtt{K}_a^{-1}(W_i)$. Since every $W'_{i'}$ is consistent there is no $W'_{i'}$ such that $\mathtt{K}_a^{-1}(W_i) \subset W'_{i'}$, and $\mathtt{K}_a(r_s^W)$ is empty. Furthermore, if there is a formula β such that $K_a\beta \wedge K_a\neg\beta \in W_i$ and $a \notin \mathcal{A}(r_i^W)$, then since $\vdash \bot \rightarrow \gamma$ and $\vdash K_a(\beta \wedge \neg\beta) \leftrightarrow K_a\beta \wedge K_a\neg\beta$, we have that from for every formula γ, $K_a\gamma \wedge K_a\neg\gamma \in W_i$.

The axioms AK3 and AK4 guarantee that every $\mathcal{K}_a$ is transitive and symmetric.

Theorem 3. *[Strong completeness for $\mathtt{Ax}_{nr}$] Every $\mathtt{Ax}_{nr}$-consistent set of formulas has a $\mathtt{Mod}_{nr}$-model.*

Proof. Let $\mathbb{M}^* = \langle R, \pi, \mathcal{A}, \mathcal{K}\rangle$ be the above defined canonical structure. We will prove that $\beta \in W_i$ iff $r_i^W \models \beta$ by induction on the rank of β where the rank function $\mathsf{rk}(\cdot)$ is defined such that

1. $\mathsf{rk}(\gamma_1) < \mathsf{rk}(\gamma)$ if γ_1 is a proper subformula of γ;
2. $\mathsf{rk}(\mathtt{E}^i\gamma) < \mathsf{rk}(\mathtt{C}\gamma)$ for every i.

This may be achieved by assigning ordinal ranks to formulas, in particular setting $\mathsf{rk}(\mathtt{C}\gamma) := \omega + \mathsf{rk}(\gamma)$. A detailed discussion of such a rank function is given in [6].

We distinguish the following cases for β:

- if β is a propositional letter, the statement is an immediate consequence of the definition of $\pi_i^{r^W}$.
- The proof in the cases when β is a negation or a conjunction is standard.
- $\beta = \bigcirc\beta_1$.
  $r_i^W \models \bigcirc\beta_1$ iff $r_{i+1}^W \models \beta_1$ iff $\beta_1 \in W_{i+1}$ iff $\bigcirc\beta_1 \in W_i$.
- $\beta = \beta_1 \mathtt{U} \beta_2$.

  Suppose that $r_i^W \models \beta_1\mathtt{U}\beta_2$. There is some $k \geqslant 0$ such that $r_{i+k} \models \beta_2$ and for every l, $0 \leqslant l < k$, $r_{i+l} \models \beta_1$. By the induction hypothesis, $\beta_2 \in W_{i+k}$, for $k \geqslant 0$, and $\beta_1 \in W_{i+l}$, for $0 \leqslant l < k$. By the construction of $\mathbb{M}^*$, we have that:

  - $\bigcirc^k\beta_2 \in W_i$, for some $k \geqslant 0$, and
  - $\bigcirc^l\beta_1 \in W_i$, for $0 \leqslant l < k$.

  Thus, by Lemma 6.[LF9], we have that $\beta_1\mathtt{U}\beta_2 \in W_i$.

  For the other direction, assume that $\beta_1\mathtt{U}\beta_2 \in W_i$. By Axiom AT4, $\mathtt{F}\beta_2 \in W_i$. Thus, $\mathtt{G}\neg\beta_2 \notin W_i$. By the definition of $\mathtt{G}$ and the construction of $\mathbb{M}^*$ it

means that $\neg(\top \mathtt{U} \neg\beta_2) \notin W_i$, and $\top \to \bigcirc^i \neg(\top \mathtt{U} \neg\beta_2) \notin W_0$. Furthermore, by Theorem 2, for some k_0,

$$\neg \left(\top \to (\bigcirc^i \neg((\bigwedge_{l=0}^{k_0-1} \bigcirc^l \top) \wedge \bigcirc^{k_0} \beta_2)) \right) \in W_0.$$

It follows that for some k_0, $\bigcirc^{i+k_0} \beta_2 \in W_0$.

Let $k_0' = \min\{k_0 : \bigcirc^{i+k_0} \beta_2 \in W_0\}$. If $k_0' = 0$, it means that $\beta_2 \in W_i$, so by the induction hypothesis $r_i^W \models \beta_2$, and $r_i^W \models \beta_1 \mathtt{U} \beta_2$. Next, let $k_0' > 0$. Then, we have that $\neg\beta_2 \in W_i, \ldots, W_{i+k_0'-1}$. Since, by Axiom AT3

$$\beta_2 \vee (\beta_1 \wedge (\bigcirc \beta_2 \vee (\bigcirc \beta_1 \wedge \ldots \wedge (\bigcirc^{k_0'-1} \beta_2 \vee (\bigcirc^{k_0'-1} \beta_1 \wedge \bigcirc^{k_0'} (\beta_1 \mathtt{U} \beta_2) \ldots) \in W_i$$

we have that $\beta_1 \in W_i, \ldots, W_{i+k_0'-1}$, $\beta_2 \in W_{i+k_0'}$, and by the induction hypothesis $r_i^W \models \beta_1$, $\ldots$, $r_{i+k_0'-1} \models \beta_1$, $r_{i+k_0'} \models \beta_2$. Thus, $r_i^W \models \beta_1 \mathtt{U} \beta_2$.

- $\beta = \mathtt{K}_a \beta_1$.

  Suppose that $\mathtt{K}_a \beta_1 \in W_i$. If $i \notin \mathcal{A}(r_i^W)$, then $\mathtt{K}_a(r_i^W)$ is empty, and trivially $r_i^W \models \mathtt{K}_a \beta_1$. So, let $i \in \mathcal{A}(r_i^W)$. Then $\beta_1 \in \mathtt{K}_a^{-1}(W_i)$, and for every $r_{i'}^{W'}$ such that $r_i^W \mathcal{K}_a r_{i'}^{W'}$ (by the definition of relation $\mathcal{K}_a$) $\beta_1 \in W_{i'}'$. By the induction hypothesis we have that $r_{i'}^{W'} \models \beta_1$ (for every $r_{i'}^{W'}$ such that $r_i^W \mathcal{K}_a r_{i'}^{W'}$), and $r_i^W \models \mathtt{K}_a \beta_1$.

  Conversely, let $r_i^W \models \mathtt{K}_a \beta_1$. If $i \notin \mathcal{A}(r_i^W)$, then obviously, $\mathtt{K}_a \beta_1 \in W_i$. So, suppose that $i \in \mathcal{A}(r_i^W)$ and $\mathtt{K}_a \beta_1 \notin W_s^j$. Then $\mathtt{K}_a^{-1}(W_i) \cup \{\neg\beta_1\}$ is consistent. Otherwise, by Deduction theorem we have $\mathtt{K}_a^{-1}(W_i) \vdash \beta_1$, and since $W_i \supset \mathtt{K}_a(\mathtt{K}_a^{-1}(W_i)) \vdash \mathtt{K}_a \beta_1$, by Lemma 6.[LK] and maximality of W_i, it follows that $\mathtt{K}_a \beta_1 \in W_i$, which is a contradiction. Thus, $\mathtt{K}_a^{-1}(W_i) \cup \{\neg\beta_1\}$ can be extended to a maximal consistent set $W_{i'}'$, such that $r_i^W \mathcal{K}_a r_{i'}^{W'}$. Since $\neg\beta_1 \in W_{i'}'$, then by the induction hypothesis $r_{i'}^{W'} \models \neg\beta_1$, and $r_i^W \not\models \mathtt{K}_a \beta_1$, which is a contradiction.

- $\beta = \mathtt{C} \beta_1$.

  Suppose that $\mathtt{C}\beta_1 \in W_i$. By Axiom AK5, for every $i \geqslant 0$, $\mathtt{E}^k \beta_1 \in W_i$, which means that every formula of the form $\mathtt{K}_{a_1} \ldots \mathtt{K}_{a_k} \beta_1$ belongs to W_i, and by the previous case, it is satisfied in r_i^W. Thus, $r_i^W \models \mathtt{E}^k \beta_1$, for every k, and $r_i^W \models \mathtt{C}\beta_1$.

  For the other direction, let $r_i^W \models \mathtt{C}\beta_1$. Suppose that $\mathtt{C}\beta_1 \notin W_i$ and $\bigcirc^i \mathtt{C}\beta_1 \notin W_0$, i.e.,

  $$\Phi_0(\bigcirc^i \mathtt{C}\beta_1, (\top)_{j \in \mathbb{N}}, (\mathtt{B}_j)_{j \in \mathbb{N}}) \notin W_0.$$

  Since $r_i^W \models \mathtt{E}^k \beta_1$, for every i, we have that:

  - every formula of the form $\mathtt{K}_{a_1} \ldots \mathtt{K}_{a_i} \beta_1$ is satisfied in r_i^W and, by the previous case, belongs to W_i,

– every formula of the form $\bigcirc^i \mathtt{K}_{a_1} \ldots \mathtt{K}_{a_i} \beta_1$ belongs to W_0, and
– for every i, $\bigcirc^i \mathtt{E}^k \beta_1 \in W_0$.

On the other hand, since $\Phi_0(\bigcirc^i \mathtt{C}\beta_1, (\top)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}}) \notin W_0$, by the construction of $\mathbb{M}^*$ we have that

$$\neg\Phi_0(\bigcirc^i \mathtt{E}^{i_0}\beta_1, (\top)_{j\in\mathbb{N}}, (\mathtt{B}_j)_{j\in\mathbb{N}})\} \in W_0$$

for some i_0, i.e.,

$$\neg \bigcirc^i \mathtt{E}^{i_0}\beta_1 \in W_0,$$

a contradiction. It follows that $\mathtt{C}\beta_1 \in W_i$.

□

Theorem 5. *[Soundness and Strong completeness for $\mathtt{Ax}_{nr+}$ and $\mathtt{Ax}_r$] The axiomatic system $\mathtt{Ax}_{nr+}$ is sound and strongly complete wrt. the class of $\mathtt{Mod}_{nr+}$-models.*

The axiomatic system $\mathtt{Ax}_r$ is sound and strongly complete wrt. the class of $\mathtt{Mod}_r$-models.

Proof. We give a sketch of the proof of this statement. First, it is well known that if Axiom [AK2] is added to $\mathtt{Ax}_{nr}$, all accessibility relations become equivalence relations, hence, from Theorem 3, it follows that $\mathtt{Ax}_r$ is sound and strongly complete wrt. the class of $\mathtt{Mod}_r$-models. Regarding $\mathtt{Ax}_{nr+}$, we first slightly change the definition of the above defined canonical structure $\mathbb{M}^*$:

- for an agent a, $a \in \mathcal{A}(r_i^W)$ iff A_a belongs to the corresponding W_i.

Axiom [AK2'] guarantees that, if $A_a \in W_i$, then $\mathtt{K}_a^{-1}(W_i) \subset W_i$, i.e., for the corresponding possible world r_i^W, $r_i^W \mathcal{K}_a r_i^W$. Furthermore, Axiom [AK2'''] implies that, if $A_a \notin W_i$, then $\bot \in \mathtt{K}_a^{-1}(W_i)$, i.e., $\mathtt{K}_a^{-1}(W_i)$ is inconsistent, and there is no consistent set of formulas which contains it. Hence, in that case $\mathcal{K}_a(r_i) = \emptyset$. Finally, from Axiom [AK2''] we obtain that, if $A_a \in W_i$, then $A_a \in \mathtt{K}_a^{-1}(W_i)$. It means that for every $r_{i'}^{W'}$ accessible by $\mathtt{K}_a$ from r_i^W, A_a belongs to the corresponding $W'_{i'}$, and that $\mathtt{K}_a\bot \notin W'_{i'}$. Thus, $\mathtt{K}_a^{-1}(W'_{i'})$ is not inconsistent, which in combination with Axiom [AK4] guarantees symmetry of $\mathcal{K}_a$. It follows that $\mathtt{Ax}_{nr+}$ is sound and strongly complete wrt. the class of $\mathtt{Mod}_{nr+}$-models. □