Probabilistic Consensus of the Blockchain Protocol

Bojan Marinković[1], Paola Glavan[2], Zoran Ognjanović[1], Dragan Doder[3], and Thomas Studer[4]

[1] Mathematical Institute of the Serbian Academy of Sciences and Arts, Serbia
[bojanm,zorano]@mi.sanu.ac.rs
[2] Faculty of Mech. Engineering and Naval Architecture, Croatia
pglavan@fsb.hr
[3] Université Paul Sabatier – CNRS, IRIT, France
dragan.doder@irit.fr
[4] University of Bern, Switzerland
thomas.studer@inf.unibe.ch

Abstract. We introduce a temporal epistemic logic with probabilities as an extension of temporal epistemic logic. This extension enables us to reason about properties that characterize the uncertain nature of knowledge, like "agent a will with high probability know after time s same fact". To define semantics for the logic we enrich temporal epistemic Kripke models with probability functions defined on sets of possible worlds. We use this framework to model and reason about probabilistic properties of the blockchain protocol, which is in essence probabilistic since ledgers are immutable with high probabilities. We prove the probabilistic convergence for reaching the consensus of the protocol.

Keywords: multi-agent systems · blockchain · temporal epistemic logic with probabilities · formal model · specification/verification

1 Introduction

Time, knowledge and uncertainty are fundamental properties of distributed systems. In order to be able to deal with these properties we need to represent them and reason about them. Reasoning about time and knowledge started, if not earlier, in the 1950s, 1960s with [9,15]. Since then, epistemic temporal logic has been applied in many fields. Particularly, it has been proven useful in analyzing message-passing based protocols in distributed computer networks [4,6,7], where a suitable semantics was proposed, and modal operators are used to express both agents' knowledge and temporal properties of actions in distributed systems. The idea of extending the epistemic logic with probability operators which enable reasoning about uncertainty seems natural and it is not new, see for example [5,16].

In this paper, we extend reasoning about temporal and epistemic properties of agents [10] with probability properties. Agents are not rigid, i.e. one agent participate as active or passive in the system. 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 [4]). Knowledge of an agent a is represented using the modal operator $\mathtt{K}_a$, that is interpreted with an accessibility relation in Kripke models. The temporal part of the logic is discrete 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 ($\mathtt{U}$). Probabilistic part is modeled by introducing probability operators of the form $\mathtt{P}_{a,\geqslant s}$, with the meaning that according to agent a some fact holds with the probability greater then or equal to s. Then both $\mathtt{K}_a$ and $\mathtt{P}_{a,\geqslant s}$, in $\mathtt{K}_a(\mathtt{P}_{a,\geqslant s}\phi)$, express together probabilistic knowledge i.e. that agent a will with probability at most s know some fact ϕ. We also introduce probabilistic common knowledge operators of the form $\mathtt{C}_s$, with the meaning that common knowledge of the probability of formula holds is at least s.

Nowadays, one of the most popular distributed protocols is the blockchain protocol [13], which is used, for example, to synchronize copies of the public ledger in the bitcoin cryptocurrency. By its nature blockchain is the probabilistic protocol [11] and every agent has its own knowledge which evaluates during the time [10]. In the formal language of our logic we formulate a theory which describes the blockchain. We illustrate expressiveness of the logic by reasoning about probabilistic consensus of agents participating in an execution of the blockchain protocol.

A blockchain is a decentralized, distributed and public digital ledger. The ledger is also immutable and ordered. It is used to record transactions across many computers with the property that transactions can be added only at the end of the ledger and a record cannot be altered retroactively, without the alteration of all subsequent blocks and the consensus of the network. All participants have a large common prefix of the ledger. A blockchain database is managed autonomously, without third authority, using a peer-to-peer network and a distributed time-stamping server. At any point of the protocol execution (round), each participant 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 string is a valid proof-of-work (PoW) with respect to m and a pointer to the last block of its current chain. If so, it extends its own local chain and broadcasts it to the all the other participants. Whenever a participant receives a chain that is longer than its own local chain, it replaces its own chain with the longer one [3,14]. It is possible, in the run of the protocol, that two transactions arrive approximately simultaneously. In that case, each participant chooses one transaction and works on it (approximately half choose the first one, and the other half the second one), keeping the other transaction. This situation is called fork. Fork is resolved in some of the next round when the next unique PoW is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

In essence the blockchain protocol is probabilistic since the ledgers change with high probabilities. Probabilistic temporal epistemic logic enables us to model and reason about probabilistic characteristics of the blockchain protocol: we are able to prove existence of the probabilistic common knowledge of agents about consensus on the common prefix of the ledger.

The paper [8] analyzes probabilistic conditions to achieve consensus on a public ledger, and presents a model theoretic approach with probabilistic constraints on runs that guarantee that (so called $\mathit{\Delta} - \Box$) common knowledge about the ledger is obtained. On the other hand, in this paper a theory which describes the blockchain is used as the starting point to prove existence of probabilistic common knowledge about the ledger. Other related papers are: [2] describes how an agent's knowledge is changed when a new block that might be added to the blockchain arrives; [10] develops a logic to analyze properties of the protocol in terms of knowledge of agents; [3,14] using cryptographic techniques prove that with the high probability honest agents have the same common prefix of the ledger.

The rest of the paper is organized as follows. In Section 2 we describe syntax and semantics for the considered temporal epistemic logic with probabilities. Section 3 describes the blockchain protocol as a theory (a set of proper axioms) of the presented logic. We prove important properties of the protocol in this section. Section 4 contains concluding remarks and directions for further work.

2 Temporal Epistemic Logic with Probabilities

2.1 Syntax

Let $\mathbb{N}$ be the set of nonnegative integers, Var a nonempty at most countable set of propositional letters, and $\mathbf{A} = \{a_1, \dots, a_m\}$, where $m \in \mathbb{N}$, a set of agents. Also, we introduce the set of propositional letters $\mathbf{A}_a = \{A_a | a \in \mathbf{A}\}$. The intuitive meaning of propositional letter A_a is that "agent a is active". The set For of all formulas is the smallest superset of $Var \cup \mathbf{A}_a$ which is closed under the following formation rules:

- $\psi \mapsto *\psi$ where $* \in \{\neg, \bigcirc, \mathtt{K}_a, \mathtt{C}, \mathtt{P}_{a,\geqslant s}, \mathtt{C}_s\}$, where $a \in \mathbf{A}$, $s \in [0,1]_{\mathbb{Q}}$
- $\langle \phi, \psi \rangle \mapsto \phi * \psi$ where $* \in \{\wedge, \mathtt{U}\}$.

The operators $\bigcirc$ and $\mathtt{U}$ are standard temporal operators Next and Until. We read the formula $\bigcirc\psi$ "ψ will hold in the next moment", and the formula $\varphi\mathtt{U}\psi$ " φ will hold until ψ becomes true. The remaining Boolean and temporal connectives $\vee$, $\veebar$, $\rightarrow$, $\leftrightarrow$, $\mathtt{F}$ ("sometimes"), and $\mathtt{G}$ ("always") are defined in the usual way. The formula $\mathtt{K}_a\psi$ denotes that the agent a knows ψ. The knowledge operator $\mathtt{E}$, which we read "everybody knows", is introduced as $\mathtt{E}\psi =_{def} \bigwedge_{a \in \mathbf{A}} \mathtt{K}_a\psi$. The operator $\mathtt{C}$ expresses common knowledge, i.e., the meaning of the formula $\mathtt{C}\psi$ is "that everyone knows that everyone knows that everyone knows... that ψ is true". The formula $\mathtt{P}_{a,\geqslant s}\psi$ represents that the probability of the formula ψ , according to agent a, is at least s. The probabilistic variants of the operators $\mathtt{K}_a$ and $\mathtt{E}$ are defined as abbreviations, in the following way:

- $\mathtt{K}_a^s\psi =_{def} \mathtt{K}_a(\mathtt{P}_{a,\geqslant s}\psi)$, and

- $\mathtt{E}_s\psi =_{def} \bigwedge_{a\in\mathbf{A}} \mathtt{K}_a^s\psi$,

while $\mathtt{C}_s$ is the operator for probabilistic common knowledge (i.e., common knowledge is that the probability of a formula is at least s). Theories are sets of formulas.

2.2 Semantics

In this paper we will consider time flow which is isomorphic to the set $\mathbb{N}$. Our models are propositional Kripke structures with possible worlds, similar as the interpreted systems from [4,16].

Definition 1. *A model $\mathcal{M}$ is any tuple $\langle W, R, \pi, \mathcal{A}, \mathcal{K}, \mathcal{P}\rangle$ such that*

- *W is the set of possible worlds,*
- *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 a set of* active agents *to each possible worlds,*
- *$\mathcal{K} = \{\mathcal{K}_i^a : a \in \mathbf{A}\}$ is the set of binary* accessibility relations *on R, such that*
  - *if $a \notin \mathcal{A}(r_i)$, then $r\mathcal{K}_i^a r'$ is false for all $r' \in R$.*
- *$\mathcal{P}$ associates a probability space $\mathcal{P}(r_i, a) = (R_{r_i}^a, \xi_{r_i}^a, \mu_{r_i}^a)$ to every possible world r_i and every agent a, such that*
  - *$R_{r_i}^a$ is a non-empty subset of R,*
  - *$\xi_{r_i}^a$ is an algebra of subsets of $R_{r_i}^a$ whose elements are called measurable sets, and*
  - *$\mu_{r_i}^a : \xi_{r_i}^a \to [0,1]$ is a finitely-additive probability measure.*

We denote the class of all models by `Mod`.

Note that in Definition 1 we consider the general case and did not introduce any restrictions on $\mathcal{K}_i^a$, except introduction of "dead end worlds" in the situations when agents are not active. In order to reason about agents' knowledge, we will consider the case when $\mathcal{K}_i^a$ are equivalence relations for the active agents.

2.3 Satisfiability relation

The satisfiability relation $\models$ is recursively defined as follows:

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

1. *$r_i \models q$ iff $\pi_i^r(q) = \top$, for $q \in Var \cup \mathbf{A}_a$,*
2. *$r_i \models A_a$ iff $a \in \mathcal{A}(r_i)$,*

3. $r_i \models \beta_1 \wedge \beta_2$ *iff* $r_i \models \beta_1$ *and* $r_i \models \beta_2$,
4. $r_i \models \neg\beta$ *iff not* $r_i \models \beta$ ($r_i \not\models \beta$),
5. $r_i \models \bigcirc\beta$ *iff* $r_{i+1} \models \beta$,
6. $r_i \models \beta_1 \mathtt{U} \beta_2$ *iff there is an* $j \geqslant 0$ *such that* $r_{i+j} \models \beta_2$, *and for every* k, *such that* $0 \leqslant k < j$, $r_{i+k} \models \beta_1$,
7. $r_i \models \mathtt{K}_a\beta$ *iff* $r'_i \models \beta$ *for all* r' *such that* $r\mathcal{K}^a_i r'$,
8. $r_i \models \mathtt{C}\psi$ *iff for every* $n \geqslant 0$, $r_i \models \mathtt{E}^n\psi$,
9. $r_i \models \mathtt{P}_{a,\geqslant s}\beta$ *iff* $\mu^a_{r_i}(\{r' \in R \mid r'_i \models \beta\}) \geqslant s$, *and*
10. $r_i \models \mathtt{C}_r\beta$ *iff for every* $n \geqslant 0$, $r_i \models \mathtt{E}^n_r\beta$.

□

Our semantic definition of probabilistic common knowledge is taken from the paper [12], where the operator $\mathtt{C}_r$ is introduced for a the first time, as reflexive and transitive closure of $\mathtt{E}_r$.[5]

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 in a model*, if it holds in every world of the model. α is *valid* ($\models \alpha$), if it is valid in each model. A formula α is a *semantic consequence* of a set of formulas F ($F \models \alpha$) if for every model $\mathcal{M}$ in which all formulas from the set F are valid, $\mathcal{M} \models \alpha$.

In order to keep the satisfiability relation well-defined, in this work we consider only so-called *measurable* models. A measurable model is a model in which each set $\{r' \in R \mid r'_i \models \beta\}$ belongs to $\xi^a_{r_i}$ for every possible world r_i and every agent a. The class of all measurable models is denoted by $\mathtt{Mod}_{Meas}$.

We consider models with non rigid sets of active atoms. We can assume that non-active agent (i.e. $a \notin \mathcal{A}(r_i)$) knows everything (i.e. $r_i \models \mathtt{K}_a\beta$, for every formula β). However, since satisfiability of knowledge of a group is represented as a conjunction of knowledge of agents from the group, knowledge of a non-active agents do not affect the knowledge of the group of active agents.

3 Blockchain Protocol

The blockchain protocol is used in the process of obtaining the consensus among the agents in distributed environment. The most known used version of the blockchain protocol is the bitcoin and some other cryptocurrencies. In this section we will describe the blockchain protocol [1,3,13,14] and provide the proof that the consensus is achieved with the high probability.

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

- It is managed autonomously, without third authority.
- It solves the long-standing problem of double spending.
- It provides a record that compels offer and acceptance, since the fact that all the transactions are kept in the public ledger.

[5] In [5], a slightly different definition is presented, and it is pointed out that both definitions are valid probabilistic generalizations of common knowledge. For the details we refer the reader to [5].

3.1 Overview of the Blockchain Protocol

In the blockchain environment transactions, that record chaining the ownership of goods between the agents in the distributed network, are kept permanently and publicly available. A transaction with the corresponding data (time stamp, identifiers of agents and value of property) are recorded in the blocks that are parts of a digital public ledger. The agents follow certain set of rules how to add and accept new blocks, add them to the ledger and achieve consensus among them. The most known version of such set of rules is so called PoW, i.e. all the agents try to solve unique cryptographic puzzle and all the agents have to accept the first valid solution. Since the fact that the hash function is used, one block in the ledger cannot be replace without the replacement of the whole section of all subsequent blocks.

The blockchain protocol was introduced in the following way (quotation from [13]):

> 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 PoW for its block.
> 4. When a node finds a PoW, it broadcasts the block to all nodes.
> 5. Nodes accept the block only if all transactions in it are valid and not already spent.
> 6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.
>
> 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 PoW is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

A round is described with the above described steps ($1-6$). Each node tries to increase the length of its own chain by “mining” the new block: find the string that will produce the hash value of the whole block that satisfies the certain property. If several blocks are produced approximately simultaneously every node can choose which branch will try to extend. This situation is called fork. Forks are resolved in later rounds, when all the nodes will accept the longest branch.

We consider the blockchain protocol that runs in a synchronous setting (the time needed to solve a puzzle for one round is much greater than the time to exchange that information among the agents). 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 Modeling of the Blockchain Protocol

The logic presented in this paper extends the temporal epistemic logic with a non-rigid set of agents from [10] to allow probabilistic reasoning. In [10] a theory (set of formulas) in the corresponding language is formulated to describe a simplified version of the blockchain protocol. The simplification concerns avoiding probabilistic behavior which characterizes the blockchain, and there is an axiom which says that forks will be resolved after a fixed number of rounds. Here we overcome this constraint since we can express explicit probabilities. We replace the mentioned axiom of the temporal epistemic logic with a new one ([AB11]) which determines the probability that after z rounds all agents have the same prefix of the ledger. As a consequence, we can consider more realistic (probabilistic) executions of the blockchain and formulate and prove a statement about probabilistic common knowledge among agents.

We define Var as $Var \supseteq \mathbf{POW} \cup \mathbf{ACC}$, where:

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

We set

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

The formulas $e_{a,i}$ mean that every active agent accepts the PoW 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 PoW produced for round i.

We will use $\mathsf{pf} \in (0, 1)$ to denote the probability that a fork occurs in a particular round.

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

AB1 $\bigvee_a A_a$
AB2 $\mathsf{acc}_{b,a,i} \rightarrow \mathsf{pow}_{a,i}$
AB3 $\mathsf{acc}_{b,a,i} \rightarrow \mathsf{K}_b \mathsf{acc}_{b,a,i}$
AB4 $\mathsf{acc}_{b,a,i} \rightarrow \neg \mathsf{acc}_{b,c,i}$, for each $c \neq a$
AB5 $\mathsf{acc}_{a,c,j} \wedge \bigcirc \mathsf{acc}_{b,a,i} \rightarrow \bigcirc \mathsf{acc}_{b,c,j}$, for $j < i$
AB6 $A_b \wedge \bigvee_a \mathsf{pow}_{a,i} \rightarrow \mathsf{ech}_{b,i}$
AB7 $\mathsf{ech}_{a,i} \rightarrow A_a$
AB8 $\mathsf{ech}_{a,i+1} \rightarrow \mathsf{ech}_{a,i}$
AB9 $\mathsf{ech}_{b,i} \rightarrow \bigcirc \bigvee_a \mathsf{pow}_{a,i+1}$
AB10 $\neg \mathsf{ech}_{a,i} \rightarrow \neg \bigcirc \mathsf{pow}_{a,i+1}$
AB11 $\mathsf{ech}_{a,i+\mathsf{z}} \wedge \mathsf{acc}_{a,b,i} \rightarrow \mathsf{P}_{a,\geqslant(1-\mathsf{pf}^{\mathsf{z}})} e_{b,i}$

Let us briefly discuss the meaning of the above axioms.

AB1 There is always at least one agent active.

AB2 One can only accept PoW that has been produced.

AB3 The agents know if they accept some PoW.

AB4 An agent accepts at most one PoW 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 PoW for a later round, then b must also accept c's PoW for round j. This essentially means that if b accepts a's PoW, 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 PoW for round $i+1$, then the agent also accepts some PoW for round i.

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

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

AB11 This states how the probability that PoW remains in the common history depends on how deep it is in the ledger. Note that we do not have any assumption on how this consensus is achieved. This formalizes the *common prefix* property from [3].

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 lenght i. Because of [AB9], at time instant $t+1$ some agent a will produce a PoW 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 PoW for round $i+1$ is generated at time instant $t+1$. It is possible that some PoW for round $i+1$ is produced at a later time instant.

The following lemmas will be used to prove the statement in Theorem 1.

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

Lemma 2. *The following holds:*

RPN: *if* $\mathbf{BCT} \models \beta$ *then* $\mathbf{BCT} \models \mathtt{P}_{a,\geqslant 1}\beta$

RICP: *if* $\mathbf{BCT} \models \mathtt{E}^i_s\beta$*, for all* $i \geqslant 0$*, then* $\mathbf{BCT} \models \mathtt{C}_\mathtt{s}\beta$

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

Lemma 3. *The following holds* $\mathbf{BCT} \models e_{a,i} \to \neg e_{b,i}$ *for* $b \neq a$.

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

Lemma 4. *We have* $\mathbf{BCT} \models e_{a,i} \to \bigcirc e_{a,i}$.

The following lemma says that if an agent accepts the choice of an another agent for a round then it accepts the whole history of that other agent.

Lemma 5. *We have* $\mathbf{BCT} \models A_b \wedge \mathsf{ech}_{a,i} \to \mathsf{ech}_{b,i}$.

For the proof of Theorem 1 we need to prove the following lemma.

Lemma 6. *If* $\mathbf{BCT} \models \alpha \to \mathtt{E}_s\alpha$, *then* $\mathbf{BCT} \models \alpha \to (\mathtt{E}_s)^k\alpha$ *for any* $k \in \mathbb{N}$.

Proof.

Suppose $\mathbf{BCT} \models \alpha \to \mathtt{E}_s\alpha$ (1)

By [RPN] $\mathbf{BCT} \models \mathtt{P}_{a,=1}(\alpha \to \mathtt{E}_s\alpha)$ for some agent $a \in \mathbf{A}$

And also $\mathbf{BCT} \models \mathtt{E}_1(\alpha \to \mathtt{E}_s\alpha)$ (2)

Further from probabilistic logic we have

$\mathbf{BCT} \models \mathtt{P}_{a,=1}(\beta \to \gamma) \to (\mathtt{P}_{a,\geqslant s}\beta \to \mathtt{P}_{a,\geqslant s}\gamma)$

for some agent $a \in \mathbf{A}$

Thus we get: $\mathbf{BCT} \models \mathtt{E}_1(\beta \to \gamma) \to (\mathtt{E}_s\beta \to \mathtt{E}_s\gamma)$ (3)

Thus 2 and 3 together (with $\beta = \alpha$ and $\gamma = \mathtt{E}_s\alpha$) yield $\mathtt{E}_s\alpha \to \mathtt{E}_s\mathtt{E}_s\alpha$

together with 1 we obtain $\mathbf{BCT} \models \alpha \to \mathtt{E}_s\mathtt{E}_s\alpha$

We can iterate this to obtain $\mathbf{BCT} \models \alpha \to (\mathtt{E}_s)^k\alpha$ for any natural number k.□

As a result of Theorem 1 we get the estimation of the probability of the consensus of an agent:

Theorem 1. *We have* $\mathbf{BCT} \models \mathsf{ech}_{a,i+\mathsf{z}} \wedge \mathsf{acc}_{a,b,i} \to \mathtt{C}_{1-\mathsf{pf}^{\mathsf{z}}}e_{b,i}$.

Proof.

For an arbitrary agent c by [AB3]: $\mathbf{BCT} \models \mathsf{acc}_{c,b,i} \to \mathtt{K}_c\mathsf{acc}_{c,b,i}$. (4)

Also, $\mathbf{BCT} \models \mathsf{acc}_{c,d,i+\mathsf{z}} \to \mathtt{K}_c\mathsf{acc}_{c,d,i+\mathsf{z}}$, and: $\mathbf{BCT} \models \bigvee\limits_{d\in\mathbf{A}} \mathsf{acc}_{c,d,i+\mathsf{z}} \to \bigvee\limits_{d\in\mathbf{A}} \mathtt{K}_c\mathsf{acc}_{c,d,i+\mathsf{z}}$,

$\mathbf{BCT} \models \bigvee\limits_{d\in\mathbf{A}} \mathsf{acc}_{c,d,i+\mathsf{z}} \to \mathtt{K}_c \bigvee\limits_{d\in\mathbf{A}} \mathsf{acc}_{c,d,i+\mathsf{z}}$,

which give us: $\mathbf{BCT} \models \mathsf{ech}_{c,i+\mathsf{z}} \to \mathtt{K}_c\mathsf{ech}_{c,i+\mathsf{z}}$. (5)

By 4 and 5: $\mathbf{BCT} \models \mathsf{ech}_{c,i+\mathsf{z}} \wedge \mathsf{acc}_{c,b,i} \to \mathtt{K}_c\mathsf{ech}_{c,i+\mathsf{z}} \wedge \mathtt{K}_c\mathsf{acc}_{c,b,i}$

and $\mathbf{BCT} \models \mathsf{ech}_{c,i+\mathsf{z}} \wedge \mathsf{acc}_{c,b,i} \to \mathtt{K}_c(\mathsf{ech}_{c,i+\mathsf{z}} \wedge \mathsf{acc}_{c,b,i})$. (6)

By [AB11]: $\mathbf{BCT} \models \mathsf{ech}_{c,i+\mathsf{z}} \wedge \mathsf{acc}_{c,b,i} \to \mathtt{P}_{a,\geqslant(1-\mathsf{pf}^{\mathsf{z}})}e_{b,i}$,

so by 6: $\mathbf{BCT} \models \mathsf{ech}_{c,i+\mathsf{z}} \wedge \mathsf{acc}_{c,b,i} \to \mathtt{K}_c^{1-\mathsf{pf}^{\mathsf{z}}}e_{b,i}$.

Using Lemma 5 we get $\mathbf{BCT} \models A_c \land \mathsf{ech}_{a,i+\mathsf{z}} \land \mathsf{acc}_{c,b,i} \rightarrow \mathsf{K}_c^{1-\mathsf{pf}^{\mathsf{z}}} e_{b,i}$.

We have that $\mathbf{BCT} \models A_c \land e_{b,s} \rightarrow \mathsf{acc}_{c,b,s}$.

Thus we obtain $\mathbf{BCT} \models A_c \land \mathsf{ech}_{a,i+\mathsf{z}} \land e_{b,i} \rightarrow \mathsf{K}_c^{1-\mathsf{pf}^{\mathsf{z}}} e_{b,i}$.

We have that $\mathbf{BCT} \models \neg A_c \rightarrow \mathsf{K}_c \bot$.

Hence we have $\mathbf{BCT} \models \mathsf{ech}_{a,i+\mathsf{z}} \land e_{b,i} \rightarrow \mathsf{K}_c^{1-\mathsf{pf}^{\mathsf{z}}} e_{b,i}$.

Since c was arbitrary, this gives us $\mathbf{BCT} \models \mathsf{ech}_{a,i+\mathsf{z}} \land e_{b,i} \rightarrow \mathsf{E}_{1-\mathsf{pf}^{\mathsf{z}}} e_{b,i}$.

Using Lemma 6 and [RICP] we finally conclude

$\mathbf{BCT} \models \mathsf{ech}_{a,i+\mathsf{z}} \land \mathsf{acc}_{a,b,i} \rightarrow \mathsf{C}_{1-\mathsf{pf}^{\mathsf{z}}} e_{b,i}$.

□

As a corollary we get the following result.

Corollary 1. *With high probability the active agents have unique common history:* $\mathbf{BCT} \models \mathsf{ech}_{a,i+\mathsf{z}} \rightarrow \bigwedge_{k=0}^{i} (\mathsf{acc}_{a,b,k} \rightarrow \mathsf{C}_{1-\mathsf{pf}^{\mathsf{z}}} e_{b,k})$.

Proof. Let $0 \leq k \leq i$. $\mathbf{BCT} \models \mathsf{ech}_{a,i+\mathsf{z}}$ and [AB8] yields $\mathbf{BCT} \models \mathsf{ech}_{a,k+\mathsf{z}}$. Theorem 1 gives $\mathbf{BCT} \models \mathsf{acc}_{a,b,k} \rightarrow \mathsf{C}_{1-\mathsf{pf}^{\mathsf{z}}} e_{b,k}$, which implies the statement. □

Corollary 1 corresponds to [3, Theorem 15], [8, Theorem 5.2] and [14, Claim 6.2]. This is, so called, *persistence* property [3]: "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." The main difference with the results given in [8] is that we can express how ledgers are evolving during the execution of the blockchain protocol, while [8] shows how a consensus between all agents can be achieved. Also, in [8] they reason about the probabilities to reach common knowledge, while here we used probabilistic common knowledge.

4 Conclusion

In this paper, we define the semantics of temporal epistemic probabilistic logic. We employ this framework to study the blockchain protocol. We prove that the blockchain protocol has the property of achieving probabilistic common knowledge among a set of agents. i.e. of reaching the consensus of the system with the high probability.

Presented description assumes that the messages are transferred between the agents much faster then the length of the period for the generation of a new PoW. We plan to develop an axiomatic system for our logic and to study proof theoretic properties of the framework. Also, another task could be to use this approach as a base ground for formal generated proof using the proof assistants like, e.g., Coq or Isabelle/HOL.

Acknowledgment

This work was supported by the Serbian Ministry of Education and Science through projects ON174026, OI174010 and III44006, the Swiss National Science Foundation 200021 165549, and by ANR-11-LABX-0040-CIMI.

References

1. K. Brünnler. *Blockchain kurz & gut.* O'Reilly, 2018.
2. 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*, 107–119, Springer, 2018.
3. J. Garay, A. Kiayias, N. Leonardos. *The Bitcoin Backbone Protocol: Analysis and Applications.* Cryptology ePrint Archive, https://eprint.iacr.org/2014/765.pdf, 2017.
4. R. Fagin, J. Halpern, Y. Moses, M. Y. Vardi. *Reasoning About Knowledge.* The MIT Press, Cambridge, Massachusetts, 1995.
5. R. Fagin, J. Halpern. *Reasoning about Knowledge and Probability.* Journal of the ACM (JACM), 41(2), 340–367, 1994.
6. J. Halpern, R. Fagin. *Modelling knowledge and action in distributed systems.* Distributed Computing 3, 159–177, 1989.
7. J. Halpern, Y. Moses. *Knowledge and common knowledge in a distributed environment.* Journal of the ACM 37:3, 549–587, 1990.
8. 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`
9. J. Hintikka. *Knowledge and Belief: An Introduction to the Logic of the Two Notions.* Cornell University Press, 1962.
10. B. Marinković, P. Glavan, Z. Ognjanović, T. Struder. *A Temporal Epistemic Logic with a Non-rigid Set of Agents for Analyzing the Blockchain Protocol.* Journal of Logic and Computation, doi:10.1093/logcom/exz007, 2019.
11. C. Mirto, J. Yu, V. Rahli, P. Esteves-Verissimo. *Probabilistic Formal Methods Applied to Blockchain's Consensus Protocol* BCRB 2018 : DSN Workshop on Byzantine Consensus and Resilient Blockchains , Luxembourg, 2018.
12. D. Monderer, D. Samet. *Approximating common knowledge with common beliefs.* Games and Economic Behavior1, 2, 170–190, 1989.
13. S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System.* `https://bitcoin.org/bitcoin.pdf`. 2009.
14. 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.
15. A. N. Prior. *Time and Modality.* Clarendon Press, Oxford, 1957.
16. S. Tomović, Z. Ognjanović, D. Doder. *Probabilistic Common Knowledge Among Infinite Number of Agents.* Proceedings of the ECSQARU 2015, LNCS 9161, 496–505, 2015.