Blockchain Safety in a Topos

Ottawa Logic Seminar

Michael Lambert

2 December 2021

Mount Allison University

Plan:

1. What is a blockchain? What is safety?
2. Forcing relative to a geometric morphism.
3. Presheaf forcing interpretation of safety.
4. Elementary forcing interpretation of safety.
5. Prospectus and Speculation

ArXiv reference: [Lam21]

Disclaimers/hedging:

1. Not a talk on programming.
2. No content here actually concerns details or implementation of consensus protocols.
3. Discussing an application of topos theory in describing well-established phenomena in comp sci, but not meant to be particularly useful to comp sci.

What is a blockchain safety?

- A **distributed system** is a network of interconnected nodes tasked with solving a computational problem.
- **Safety** in a distributed system is a guarantee that "nothing bad will happen" [Lam77].

- A blockchain is a public ledger managed by a distributed system. Features:
  1. composed of individual blocks: each has an ID hash, each identifies a unique immediate predecessor, and each contains network transaction data
  2. should ultimately be a linear order of blocks
  3. latency, down or faulty nodes, malicious actors $\rightsquigarrow$ blocks minted simultaneously or with conflicting data.
- Network needs to reach **consensus** concerning which blocks to include and which to throw out. "Fork choice" or "forking."
- Blockchain **protocol** governs how nodes communicate, how blocks are minted, how consensus is reached.
- peer-to-peer $\approx$ no central authority, just the protocol
- Examples: Bitcoin, Ethereum, Cardano, Algorand etc.

- Blockchain consensus safety: the protocol will not validate blocks with conflicting data.
- "Validate" $\approx$ accept certain blocks in fork choice.
- Goal: design a template for consensus protocols from which safety is *provable* as a feature. Ref: [Zam17]

Estimate Safety

- Abstract template for Ethereum blockchain [Zam17]
- Let Σ denote a category: objects are protocol states; arrows are executions/state transition: "do something"
- C is a set of "consensus values" $\approx$ a hypothetical totality of all blockchain configurations
- $E : \Sigma \to PC$ an "estimator" assigning to each state an estimate as to the configuration of the blockchain $\approx$ fork choice in a given state.
- E satisfies a technical condition.

- **Definition.** A proposition $p \in PC$ is **safe** in state $w \in \Sigma$ if $Ev \leq p$ for all executions $w \to v$.
- **Safety Theorem.** [Zam17] Any proposition and its negation cannot be safe in states with a common future state: it is not the case that p is safe in w_1 and $\neg p$ is safe in w_2 if there are executions $w_1 \to w_3 \leftarrow w_2$.
- Theorem is provable without appeal to DeMorgan or excluded middle, and makes sense for any contradictory propositions. Topos logic?
- Forcing mojo: p is safe at w if it is forced at w to be in the fork choice of every subsequent protocol state. Kripkean!

Presheaf Forcing Semantics

- Let $F\colon \mathscr{C} \to \mathscr{D}$ denote any functor. Think $E\colon \Sigma \to PC$.
- Induces a geometric morphism $F\colon [\mathscr{C}, \mathbf{Set}] \to [\mathscr{D}, \mathbf{Set}]$.
- Notation: $H^* = F^*H$ and $K_* = F_*K$. In particular $\Omega_* = F_*\Omega$.
- Let $\phi\colon X \to \Omega_*$ be any morphism, $C \in \mathscr{C}$ and $a \in F^*X$. Let $\bar{\phi}$ be its transpose $\bar{\phi} = \epsilon\phi^*\colon X^* \to \Omega$.
- Define: $C \Vdash_* \phi(a)$ if, and only if, $C \Vdash \bar{\phi}(a)$ holds.
- That is, $C \Vdash_* \phi(a)$ if, and only if, $a \in S_{\bar{\phi}}C$.
- See §4 [AKK14] for original relation in special case $|\mathscr{C}| \to \mathscr{C}$.

Lemma
$C \Vdash_* \phi(a)$ holds if, and only if, $D \Vdash_* \phi(f_! a)$ for all $f : C \to D$.

Proof.

$$
\begin{aligned}
C \Vdash_* \phi(a) &\equiv C \Vdash \epsilon\phi^*(a) \\
&\equiv \epsilon\phi^*(a) = \top_C \\
&\equiv \{f : C \to D \mid f_!(a) \in S_{\epsilon\phi^*} D\} = \mathfrak{t}_C \\
&\equiv f_!(a) \in S_{\epsilon\phi^*} D \text{ for all } f : C \to D \\
&\equiv \epsilon\phi^*(f_!(a)) = \top_D \text{ for all } f : C \to D \\
&\equiv D \Vdash \epsilon\phi^*(f_!(a)) \text{ for all } f : C \to D \\
&\equiv D \Vdash_* \phi(f_!(a)) \text{ for all } f : C \to D
\end{aligned}
$$

□

- A **geometric model** is a surjective geometric morphism $F : \mathscr{F} \to \mathscr{E}$ (i.e. F^* is faithful)
- F is a geometric model if, and only if, $\Omega_{\mathscr{E}} \to \Omega_*$ is monic
- semantics of $\Vdash_*$ and $\Box$-operator are especially well-behaved for geometric models
- $F : \mathscr{C} \to \mathscr{D}$ induces a geometric model $F : [\mathscr{C}, \mathbf{Set}] \to [\mathscr{D}, \mathbf{Set}]$ if, and only if, every object of $\mathscr{D}$ is a retract of one in the image of F
- $E : \Sigma \to PC$ induces a geometric model iff surj. on obj.

Presheaf Forcing Interpretation Setup:

- suppose that $E : \Sigma \to PC$ surjective on objects
- let $p \in PC$ be given
- identify p with the support of the corresponding representable functor in $[PC, \mathbf{Set}]$
- classifying map $\chi_p : 1 \to \Omega$ in $[PC, \mathbf{Set}]$
- consider the composite $i\chi_p$ where $i : \Omega \to \Omega_*$ unique frame homomorphism (i monic!)

Theorem
A proposition $p\colon U \to 1$ *is safe in state* w *if, and only if,* $w \Vdash_* i\chi_p$.

Proof.

$$\begin{aligned} w \Vdash_* i\chi_p &\equiv v \Vdash_* i\chi_p \text{ for all } w \to v \\ &\equiv v \Vdash \overline{i\chi_p} \text{ for all } w \to v \\ &\equiv v \leq S_{\overline{i\chi_p}} \text{ in } \mathrm{Sub}_{\mathscr{F}}(1) \text{ for all } w \to v \\ &\equiv ev \leq p \text{ in } \mathrm{Sub}(1)_{\mathscr{E}} \text{ for all } w \to v \\ &\equiv ev \Rightarrow p = \top \text{ in } \mathrm{Sub}(1)_{\mathscr{E}} \text{ for all } w \to v. \end{aligned}$$

Penultimate step: the transpose of $S_{\overline{i\chi_p}}$ is isomorphic to p because p is classified by $i\chi_p$ since i is monic. □

Denote by $\Box\phi$ the composite

$$X \xrightarrow{\phi} \Omega_* \xrightarrow{\tau} \Omega \xrightarrow{i} \Omega_*$$

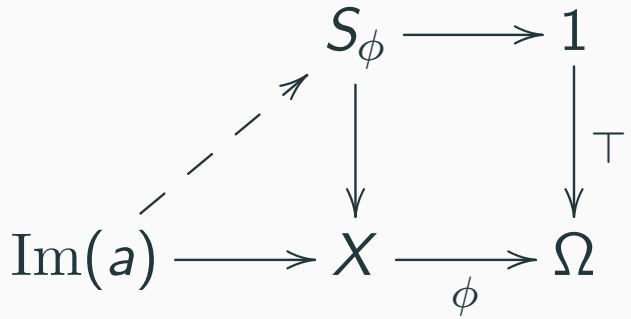
where τ is the classifying arrow of $\top_* \colon 1 \to \Omega_*$ (cf. [AKK14]).

Corollary
$p \colon U \to q$ is safe in w if, and only if, $w \Vdash_* \Box i\chi_p$.

Proof.
$w \Vdash_* \Box i\chi_p$ iff $w \Vdash_* i\chi_p$ since i is monic. Now use the theorem. □

Elementary Interpretation

- work in a topos $\mathscr{E}$ (not necessarily Grothendieck)
- recall forcing relation: A morphism $a\colon W \to X$ **forces** $\phi\colon X \to \Omega$ if



  equivalently $\phi(a) = \top_W$
- denote this by $W \Vdash \phi(a)$

Definition
An **estimate consensus protocol** *in a topos* $\mathscr{E}$ *consists of*

1. *an object* C *of consensus values;*
2. *an internal category* Σ *of states* Σ_0 *and executions* Σ_1*;*
3. *an internal functor* $e\colon \Sigma \to PC$ *called the* **estimator** *satisfying: if* $e(w) \Rightarrow p = \top$ *for some state* $w\colon X \to \Sigma_0$*, then* $\neg(e(w) \Rightarrow \neg p) = \top$ *for any proposition* $p\colon 1 \to PC$*.*

Definition
A proposition $p\colon 1 \to PC$ *is* **safe in the protocol state** $w\colon W \to \Sigma_0$ *if for any execution* $f : w \to v$*, it follows that* $ew \Rightarrow p = \top$ *holds.*

For any state $w\colon W \to \Sigma_0$, form the object of executions from w as the pullback

$$\begin{array}{ccc} \Sigma(w,-) & \longrightarrow & \Sigma_1 \\ \downarrow & & \downarrow{\scriptstyle d_0} \\ W & \xrightarrow[w]{} & \Sigma_0. \end{array}$$

For any execution $f\colon w \to v$ on w, that is,

$$\begin{array}{ccc} X & \xrightarrow{f} & \Sigma_1 \\ \downarrow & & \downarrow{\scriptstyle d_0} \\ W & \xrightarrow[w]{} & \Sigma_0 \end{array}$$

there is a unique morphism $\hat{f}\colon X \to \Sigma(w,-)$ i.e. f is an element of the "fiber" of the reprentable functor at $v \in \Sigma_0$.

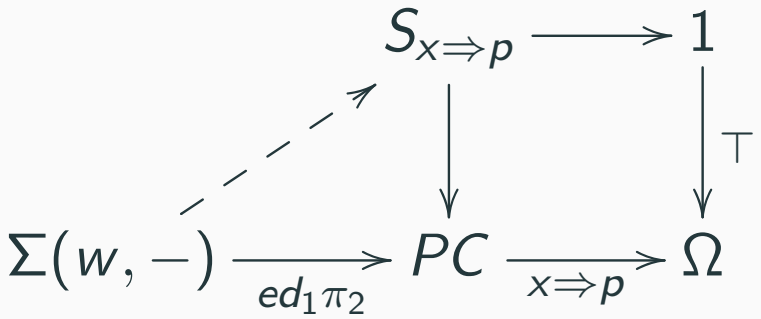
For any proposition $p\colon 1 \to PC$, form the implication $x \Rightarrow p$ for a variable $x : PC$ as the composite

$$PC \cong PC \times 1 \xrightarrow{x \times p} PC \times PC \xrightarrow{\Rightarrow} \Omega$$

where '$\Rightarrow$' classifies $(\leq) \to PC \times PC$. Identify w with the representable $\Sigma(w, -)$ in the forcing notation. That is, write '$w \Vdash x \Rightarrow p$' as a shorthand for '$\Sigma(w, -) \Vdash x \Rightarrow p$'.

Theorem
$p\colon 1 \to PC$ is safe in w if, and only if, $w \Vdash (x \Rightarrow p)(ed_1)$.

Proof.
($\Rightarrow$) Assume safety: $ed_1\pi_2\colon \Sigma(w,-) \to PC$ satisfies $ed_1\pi_2 \Rightarrow p = \top$. Then



($\Leftarrow$) Assume $ed_1\pi_2 \Rightarrow p = \top$ holds. Any f factors through $\Sigma(w,-)$ via $\hat{f}\colon X \to \Sigma(w,-)$ satisfying $\pi_2\hat{f} = f$. Thus, compute that $\top = ed_1\pi_2\hat{f} \Rightarrow p = ed_1 f \Rightarrow p = ev \Rightarrow p$. $\square$

In this topos-setup, can prove the main safety result:

Theorem (Estimate Safety)
Inconsistent propositions are not safe at related states. That is, if $p \wedge q = \bot$ *and* $w_1 \simeq w_2$ *both hold, then it is not the case that both* $w_1 \Vdash (x \Rightarrow p)$ *and* $w_2 \Vdash (x \Rightarrow q)$ *hold.*

This depends on some lemmas. See [Lam21] for full version.

Prospectus/Musings

- no mention of protocol Σ
- this is the point of the template: from any $E : \Sigma \to PC$, a safety result should be provable
- "safety" originates in distributed computing [Lam77]
- I/O automata as formal models
- safety shows up in other contexts

Example: Gödel Translation

- topology: upward closed subsets of a poset X
- include $\mathscr{O}(X) \to PX$
- $p \in PX$ is **safe** in state $x \in X$ if $x^{\uparrow} \subset p$
- "*safely*(p)" $=$ modal operator
- ref: [Kis18]
- general situation: Garner's ionads?

Speculative Example: Spacetime Logic

- future of an event = cone of "accessible events"
- event p is **safe** for event x if p is in the future of every event in the future of x
- Minkowski spacetime logic = S4 modality [Gol80]
- spacetime logic formulable in terms of non-deterministic cellular automata (deep lore?)

Closing Thoughts:

- automata models in indexed categories [Jaz20]
- distributed computing $\cap$ concurrency $=$ nontrivial
- directed type theory $\rightsquigarrow$ models of concurrency [Nor18]; needs comprehension scheme [Jac93] for interpretation
- big leap: fibration models as setting for forcing interpretation of safety formalized in nondeterministic automata
- application of double categories: probably need a bifibration to interpret connectives and an involution $(-)^{op}$ for directedness; i.e. need a special kind of equipment [Shu08]

THANK YOU!

References


Steve Awodey, Kohei Kishida, and Hans-Christophe Kotzsch.
Topos semantics for higher-order modal logic.
Logique et Analyse, 57(228):591–636, 2014.


Robert Goldblatt.
Diodorean modality in minkowski spacetime.
Studia Logica: An International Journal for Symbolic Logic, 39(2/3):219–236, 1980.


Bart Jacobs.
Comprehension categories and the semantics of type dependency.
Theoretical Computer Science, 107(2):169–207, 1993.

David Jaz Myers.
Double Categories of Open Dynamical Systems (Extended Abstract).
arXiv e-prints, page arXiv:2005.05956, May 2020.

Kohei Kishida.
Categories and modalities.
In Elaine Landry, editor, *Categories for the Working Philosopher*, pages 163–222. Oxford University Press, 2018.

Leslie Lamport.
Proving the correctness of multiprocess programs.
IEEE Transactions on Software Engineering, SE-3(2):125–143, 1977.

Michael Lambert.
A Topos View of Blockchain Consensus Protocols.
arXiv e-prints, page arXiv:2111.07461, November 2021.

Paige Randall North.
Towards a directed homotopy type theory.
arXiv e-prints, page arXiv:1807.10566, July 2018.

Mike Shulman.
Framed bicategories and monoidal fibrations.
Theory and Applications of Categories, 20(18):650–738, 2008.

Vlad Zamfir.
A template for correct-by-construction consensus protocols.
github, 2017.