Blockchain Cohomology

Wyatt Meldman-Floch

February 17 2018

Abstract

We follow existing distributed systems frameworks employing methods from algebraic topology to formally define primitives of blockchain technology. We define the notion of cross chain liquidity, sharding and probability spaces between and within blockchain protocols. We incorporate recent advancements in synthetic homology to show that this topological framework can be implemented within a type system. We use recursion schemes to define kernels for smooth manifolds across homotopy groups within the homology group of the topological space of a blockchain protocol.

1 Consensus Protocols

A blockchain protocol can be described in terms of the topological definitions of distributed computing as defined by T. Nowak [1]. We first define an execution space as a topological space equipped with a discrete product topology[2]. Defining a distributed process in terms of topology only requires us to care about the structure of the set of possible schedules of a distributed system[3]. We adopt Nowak's algebraic definition of an execution space in terms of the homology of protocol complexes [4]. We define a protocol complex $P_k\Delta^q$ as the q-dimensional standard simplex

$$\Delta^q = \{x \in \mathbb{R} | \Sigma x_j = 1, x_j \geq \forall j\} \tag{1}$$

at morphism k

$$P_k = \{v_{i,0} \dots v_{i,q}\} \tag{2}$$

[1] "Topology in Distributed Computing" University of Vienna

[2]

[3] Saks, Michael and Fotios Zaharoglou 2000, impossibility of the wait free k-set agreement

[4] http://www.lix.polytechnique.fr/ goubault/papers/sv.pdf

where $i \in \Sigma$ and $P \subset \Sigma \subset \mathbb{N}$ is the set of all admissible configurations.

We define a consensus protocol $H_k(S) : \{S_k, \partial_k\}$ as a chain complex of singular homology of the simplicial complex carried by a homotopy preserving group morphism (functor) implementing distributed consensus where S_k is the simplex of a protocol complex with configuration k and ∂_k is the differential of this morphism:

$$H_k(S) \equiv \dots S_{k-1} \xleftarrow{\partial_{k-1}} S_k \xleftarrow{\partial_k} S_{k+1} \dots \tag{3}$$

Formally we define our homotopy preserving group morphism implementing distributed consensus $\sigma : \Delta^q \to S$ as the singular n-simplex[5]

$$\sigma_k : S_{k-1} \times \Sigma \to S \tag{4}$$

which are continuous on discrete topologies[6] such as Δ^q. We define the homology between protocol complexes as a measure of divergence given by our differential

$$\partial_k(\sigma) = \sum_{k=0}^{q} (-i)^{i-1} (\sigma \circ \delta_q^i) \tag{5}$$

for continuous functions $\delta_q^i : \Delta^{q-1} \to \Delta^q | 1 \leq i \leq q+1$ where

$$\delta_q^i(x_1, \dots, x_q) = (x_1, \dots x_{i-1}, 0, x_i, x_{i+1}, \dots, x_{q-1}, \dots, x_q) \tag{6}$$

As the graded abelian group of our protocol complex is the simplicial singular homology group and σ is our homotopy preserving map, it is trivial to note that the homology of a protocol complex is

$$\partial_k \circ \partial_{k+1} = 0 \tag{7}$$

As a corollary of the fact that the geometric realization of a simplicial complex is dually a topological space, due to the vanishing cohomology up to k, we note that $P_k \Delta^q$ is k-acyclic[7].

2 Protocol Topologies

It's possible that we could 'mix' protocol complexes defined as above. We employ our notion of cohomology to define a 'liquidity' or the ability to exchange

[5]

[6] Lemma 4.5 Nowak

[7] Definition 5.4, Nowak

configuration states between protocol complexes. We leave applications of this as an exercise for the reader.

We define liquidity as the existence of a functoral vertex map between singular homologies (defined equivalently here as the disjoint subset of protocol complexes) $l : \bigcup_k P_\theta \to \bigcup_k P_{\theta+1}$.

Making use of homotopy type theory allows us to focus on structure by treating topological characteristics called homotopy groups as primitives. If we redefine our k-acyclic distributed consensus protocol σ categorically as the functoral carrier Σ_* we can form a chain complex that adheres to the homology theory of homotopy types.

Simplicial complexes together with simplicial vertex maps form a category. Let us define a protocol topology $T_\theta^\Sigma\ \Sigma_* P_\theta$ as the singular homology of a chain complex of protocol complexes carried by a homotopy preserving functor Σ_*. The protocol topology is given by the following chain complex

$$T_\theta^\Sigma : 0 \leftarrow \Sigma_* P_\theta \xleftarrow{\partial} \Sigma P_0 \xleftarrow{\partial} \dots \Sigma P_\theta \tag{8}$$

For protocol complex morphisms $\Sigma_\theta, \Sigma_{\theta+1}$ chain homotopy from Σ_θ to $\Sigma_{\theta+1}$ is a homotopy preserving graded abelian group morphism $l : P_\theta \to P_{\theta+1}$ yielding a vanishing homology, i.e.

$$\begin{aligned} \Sigma_\theta - \Sigma_{\theta+1} &= \partial^\theta \circ l + l \circ \partial^{\theta+1} \\ &= \partial^\theta \circ \partial^{\theta+1} = 0 \end{aligned} \tag{9}$$

Noting that these conditions are met by the definitions of an acyclic carrier [8], it follows that a protocol topology as defined above is θ-acyclic.

3 Block Sheaves

Designing distributed architectures with topology gives us a lot of power, but in order to use it we need to design our topologies such that they are mathematically tractable for solving a specific problem. In principle, Abstract Differential Geomoetry (ADT) admits any topological space for base space on which to solder the relevant sheaves[9] and carry out differential geometry upon[10] . We

[8] Nowak, Theorem 5.1

[9]

[10] ripped from millans

introduce methods from Abstract Differential Geometry, namely finitary cech-deRham cohomology in order to define a protocol topology as an orientable manifold, and use this formulation to engineer a class of blockchain scalability solutions.

First we need to introduce the dual of homology as described above, namely cohomology. In describing our protocol complex it only makes sense to have an arrow moving 'forward in time' as consensus itself is acyclic. In this sense our evolution was the compounding dimensionality of the space of all configurations, as implied by the discrete product topology of a protocol complex. In defining an orientable manifold, we need to move 'backwards' through our space, i.e. from higher to lower dimension. This is shown as the differential on an arrow going right instead of left.

By constructing the protocol topology within a monoidal category, the singular cohomology of a protocol topology is equivalent to an A-module of Z+-graded discrete differential forms. One can, in a natural way, assign a decision tree to any set of executions that captures the decision of choosing a successor. A blockchain can be defined as an extension of an execution tree, where each block is formulated as a sheaf with a well defined tensor operation. We define a sheaf ϵ as the 'enrichment' of any cochain $\mathbb{A}$-complex of positive degree/grade, corresponding to the $\mathbb{A}$-resolution of an abstract $\mathbb{A}$-module

$$S^* : 0 \to \epsilon \to S^0 \xrightarrow{d^0} S^1 \xrightarrow{d^1} \dots \tag{10}$$

and homomorphism given by Cartan-Kahler-type of nilpotent differential operator d. We will make use of the fact that an $\mathbb{A}$-module sheaf ϵ on any arbitrary topological space admits an injective resolution per (10).

Blockchains are naturally equipped with a sheaf, that of the block. This would allow us to 'unpack' data in block recursively under the product operation. Every abelian unital ring admits a derivation map [11], thus if we redefined our definition of protocol complex above as sheaves with semigroup operations carried by right derived functors with monadic bind, we can form a protocol manifold as defined below.

By redefining Sorkin's fintoposets[12] as simplicial complexes, Mallios et al. showed that the Gelfand duality[13] implies that a manifold can be constructed out of the incidence Rota algebra of a simplex's corresponding fintoposet [14]. For a fintoposet, it's incidence algebra can be broken down into a direct sum of vector subspaces

$$\Omega(P) = \bigoplus_{i \in \mathbb{Z}_+} \Omega^i = \Omega^0 \oplus \Omega^0 \cdots := A \oplus R \tag{11}$$

[11] Ka?hler
[12]
[13]
[14]

where $\Omega(P)$s are $\mathbb{Z}_+$ graded linear spaces, A is a commutative sub algebra of Ω and $R := \bigoplus_{i\geq 1} \Omega^i$ is a linear (ringed) subspace. It is trivial to notice that $\Omega(P)$ is an A-module of a Z+-graded discrete differential form.

A manifold can be constructed by organizing the incidence algebras of our protocol complexes into algebra sheaves. The n-th (singular) cohomolgy group $H_n(X, \epsilon)$ of an A-module sheaf $\epsilon(X)$ over topological space X, can be described by global sections $\Gamma_X(\epsilon) \equiv \Gamma(X, \epsilon)$

$$H_n(X, \epsilon) := R^n(\Gamma(C, \epsilon) := H^n[\Gamma(C, S^*)] := ker\Gamma_X(d^n)/im\Gamma_X(d^{n-1}) \quad (12)$$

where $R^n\Gamma$ is the right derived functor of the global section functor $\Gamma_x(.) \equiv \Gamma(X, .)$. Note that R^n is equivalent to the i^{th} linear ringed subspace above. These dual definitions of gamma correspond to out definitions of σ and Σ_* with respect to our functoral vertex map l in our definition of a protocol topology.

The corresponding abstract $\mathbb{A}$-complex S^* can be directly translated by the functor Γ_x to the 'global section $\mathbb{A}$-complex' $\Gamma_X(S^*)$

$$\Gamma_X(S^*) : \Gamma_X(0) \xrightarrow{\Gamma_X(d^0)} \Gamma_X(S^0) \xrightarrow{\Gamma_X(d^1)} \dots \quad (13)$$

$\Gamma_X(S^*)$ is abstract de Rham complex of a discrete manifold. The sheaf cohomology of a topological space is the cohomology of any Γ_X-acyclic resolution of ϵ[15].

The finitary de Rham theorem defines a finitary equivalent of the typical c^∞ smooth manifold. Noting $\Gamma_m^{P_m}$ is fine by construction, Mallios et al. show that finsheaf-cohomology differential tetrads

$$\tau := (P_m, \Omega_M, d, \Omega^M_{deR}) \quad (14)$$

is equivalent to the c^∞-smooth Cech-de Rham complex. In our defiition of τ, Ω is the categorically dual finsheaf (finitary sheaf) of Sorkin's (simplexes, equivalent) fintoposets P_m, d is effectively an exterior product, and Ω^M_{deR} is the abstract de Rahm complex. The action of d is to effect transitions between the linear subspaces Ω_i of $\Omega(P)$ in (11), as follows: d: $\Omega_i \to \Omega_i + 1$.

4 Blockchain Cohomology

We've shown how to create a manifold from the cohomology of the discrete topological space of a protocol complex. Now we show how define a synthetic manifold of multiple protocol complexes. Isomorphic to the construction of the protocol topology, we define a cochain complex within the cohomology theory of homotopy types under the cup product.

[15] the abstract de Rham theorem

Making note of the definition of a tensor product given by the Cohen et al. [16] we define the protocol manifold M as

$$\Gamma_{\theta}^{\Sigma} = \bigoplus_{0 \leq i \leq \theta} \Gamma^{*} P_i \tag{15}$$

5 Typesafe Poincare Duality

Up until now we have not explicitly defined functoral homeomorphisms that can construct the complexes described above. We show that the dual nature of the hylomorphic and metamorphic morphic recursion schemes maintain vanishing differentials and thus poincare duality for all θ.

If we define a catamorphism and anamorphism with the same f-algebra and f-coalbegra, we can show by construction that the resulting co/chain-complexes are valid definitions of protocol topologies/manifolds and that poincarre duality of the protocol manifold is maintianed up to θ isomorphism.

6 Remarks

It would be really cool if I could hand wavedly show that the protocol topology and protocol manifold make a cell in a greater cell complex.

[16]