Blockchain Cohomology

Wyatt Meldman-Floch

February 17 2018

Abstract

We propose a blockchain cohomology theory based on the homology theory of homotopy types and use this to describe the fundamental features of the constellation blockchain.

1 Blockchain Homotopy

Lets start with a super simple type theoretic definition of a blockchain. Let A be a type representing a transaction, B represent the type of a block and $\rightarrow$ represent distributed consensus, let us define a blockchain by the following construction

$$A \xrightarrow{consensus} B \tag{1}$$

If we define A and B as covariant subtypes of a universal type U, we can say that this blockchain is described by the homology theory of homotopy types. The magic that allows us to go from a simple type theoretic definition to homology is the notion of homotopy. Where π_U is the homotopy group of our universal type and Cov is covariance, homomorphism if given by

$$Hom_{A,B} = Cov(A, B) \cong \pi_B \tag{2}$$

Now why does any of this matter? It matters because we now have a formal body of mathematical machinery with which we can build complex distributed ledgers. This allows us to formally define and different blockchains the same way we engineer fields in physics. This process is known as guage theory and constitutes the formation of a gauge field. However for our purpose, it shows us how to create sessionized streams of factual data using the tools of cohomology and sheaf theory. Cohomology in our case is measure of the deviation from homotopy, or how type A and B deviate under covariance. We now define the constellation blockchains in terms of the notion of a chain complex within the homology theory of homotopy types.

2 Chain Complexes and the Constellation Blockchain

There's an annoying problem about our arrow above, which is that there's only a fixed number of A's that can be turned into a B. The constellation blockchain is a solution to this problem.

Using our type theoretic definition above, we can extend this notion of homotopy that connects A and B to create a chain complex, which for our purposes is an incrementally bigger blockchain. We define the constellation blockchain as a chain complex

$$C_R = R_0 \xrightarrow{h_0} R_1 \dots R_{n-1} \xrightarrow{h_{n-1}} R_n \tag{3}$$

where $R_{0\dots N}$ are monads "carrying" blocks of type U and $h_{0\dots n-1}$ is a special type of consensus operator called a hylomorphism which preserves homotopy.

2.1 Hylochain and Polymorphic Validation

What allows us to construct C_R is the homotopy equivalence between blocks B and the transactions they're composed of, A. Since we described blockchains in terms of homotopy type theory, we used tools from category theory to define C_R, namely the notion of a monad, and recursion schemes.

2.1.1 The Constellation DAG

The Constellation chain complex C_R is implemented as a directed acyclic graph of monads called Radials. The topological sorting of this DAG gives us the homology group of our topological space [1]

$$Hom = \{\pi_0 \dots \pi_n\} \forall n \in \mathbb{N}$$

where π_n us the homotopy group of order n

2.1.2 Radial Simplex

As a blockchain is a distributed system, we can describe our simplex R_N as a cluster of nodes partitioned into clique complexes.

Note we are forming a chain complex of monads. Those monads are implemented as simplicial complexes from which blocks are created. In this sense we are creating a cw-complex both of homotopy types and of simplexes. This allows us to define a partitioning logic for nodes to come and go from radials separate from the nodes themselves. the way we do this is by implementing the monads in terms of re ursion schemes. We define mappings between simplices in terms of the ypes of the hylomorphism. Implementing the simplicial chain complex using recusion schemes allows us to define a simplicial complex with the ease of type safety. We merely bake the rules into the type of the blocks. Specifically, instead of trying to describe this all in terms of simplicial complexes, we use the fact

[1] https://arxiv.org/pdf/1605.07798.pdf

that we can form a Serre fibration or a weak fibration, using homotopy type theory which effectively allows us to encode the logic for our dynamically partitioned network within the blocks themselves. The way we do that is by constructing our blocks as sheaves

The clique complex of a graph G is a simplicial complex whose simplices are the cliques of G[2]. We define a simplex σ as a completely connected graph (clique) of nodes, with which we can perform cryptographic consensus. Given $\sigma = \{n_0 \dots n_i\}$, σ is a Radial simplex iff:

1: σ is a complete graph such that for a set of edges e, corresponding to nodes n,

$$\forall n \in \sigma, \exists e \in E \mid e \equiv \sigma \setminus \{n\} \tag{4}$$

Corollary: for each n in a a simplex σ_K, the simplicial star[3] of n, $st_K(n)$, for simplex K is equivalent to the σ_K that is:

$$\forall n \in \sigma_k, st_K(n) \equiv \sigma_K \tag{5}$$

2: There exists a deterministic mapping given by an immutable generating function g

$$\exists g : \sigma \to d, \mid d \subseteq \sigma \tag{6}$$

3: There exists the notion of a star cluster[4] Such that star cluster σ forms an independence complex of K.

$$SC(\sigma_k) = \bigcup_k st(n) \in I_G \ \forall k \in K \tag{7}$$

Where I_G is the set of all independence graphs of K[5]. It follows from corollary (4) that

$$\begin{aligned} SC(\sigma_k) &= \bigcup_k st(n) \\ &\equiv st(n) \ \forall n \in k \end{aligned} \tag{8}$$

A hypergraph represents an arbitrary set of subsets of it a graph's vertex set, where each subset is called a edge[6]. We define the the Radial abstract data type in terms of a hypergraph and mappings between vertex sets within that hypergraph. Specifically for given Tier $t \in \mathbb{N}$ (see above), we define the Radial monoid[7] R_t as a functor[8] over the category of simplexes such that

[2]https://arxiv.org/pdf/1007.0418.pdf
[3]Closure, star, and link: wikipedia/Simplicialcomplex
[4]https://arxiv.org/pdf/1007.0418.pdf
[5]Definition 2.1 https://arxiv.org/pdf/1007.0418.pdf
[6]Pal S. et. al. http://www.facweb.iitkgp.ernet.in/ spp/geomgraph.pdf
[7]https://ncatlab.org/nlab/show/monoid
[8]https://typelevel.org/cats/typeclasses/functor.html

$$
\begin{aligned}
&R_k^n : \\
&\quad starCluster : \{R_0^{n-1} \dots R_j^{n-1}\} | j \subset k, \\
&\quad state : \{A\}, \\
&\quad hyperplane : \{n_0 \dots n_k\}_{n-1} \to \{n_0 \dots n_k\}_n,
\end{aligned}
$$

The hypergraph for all simplexes σ_k within Order O is given by the two element set

$$H_{t,k} = \{I_{g_{t-1}} \mid g_{t-1} \subset G_{t-1}, \sigma_k\} \tag{9}$$

where $I_{g_{t-1}}$ is a subset of all simplexes in tier $t-1$ (as we know all simplexes are independent) and $\sigma_k \in R_t.simplices$. $hyperPlane$ is a function that maps between two hyperedges, potentially across tiers. Note that $Sigma[T-1]$ and $I_{g_{t-1}}$ are equivalent via homotopy as shown in Defnition 2.1 (footnote 5).

In the degenerate case of our definition of R_T, namely when $R_t = \{R_0\}$, $starCluster$ is a mempool as defined below, or the set of all states shared amongst σ_k.

2.2 Typesafe Cross-chain Atomic Swaps

2.2.1 Definition of chain liquidity

Two chain complexes are chain equivalent if there exists a homotopic mapping between them. We show how homotopy is constructed for a chain complex.

Proof: we know due to the univalence axiom that homotopy is implicit from type equivalence. We know from R. Grahm that a function from $||colim_i(X_i, \theta_i)||_0 \to ||colim_i(X_i, \phi_i)||_0$ where each X_i, Y_i is a set, it suffices to show that $f_i : X_i \to Y_i$ such that $f_i \circ \phi_i = \theta_i \circ f_{i+1}$.

Thus we show that for two chain complexes with type equivalent functors, if their f-algebras are isomorphic, it follows that [9] (we can easily show with cw-complex, should add diagram)

$$f_i \circ \phi_i = \theta_i \circ f_{i+1} = \theta_i \circ f_i = \theta_i \circ \phi_i \tag{10}$$

A tensor defines chain mappings[10] and a path differential of 0 is required for homotopy. We do not have additivity which is required for a tensor, but we can get around this via the Exactness Axiom. We know that the path differential is 0 under type equivalence due to the univalence axiom, thus there exists homotopy.

Liquidity between multiple chains is isomorphic to the existence of a fibration, which is defined as $C : S \to Type$ where C is a base type, and

[9] https://www.seas.upenn.edu/ jean/sheaves-cohomology.pdf

[10] http://www.math.uni-frankfurt.de/ johannso/SkriptAll/SkriptTopAlg/SkriptTopChain/algtop4.pdf

S is a pointed set. This is analogous to classical topology where C and S are spaces. Due to the behavior of truncated colimits of sets[11] it can be shown that for $||colim_i(Y_i, \theta_i)||_0 \to ||colim_i(Z_i, \zeta_i)||_0$ given a $g_i : Y_i \to Z_i$ then $||colim_i(X_i, \theta_i)||_0 \to ||colim_i(Z_i, \zeta_i)||_0$ is given by $f \circ g$. If f, g are isomorphic then there exists a homotopy and there exists a fibration. It follows that more complicated cross chain structures can be formed by mapping cones and mapping cylinders.

2.3 Chain fibering: Scaling through Recursive Parachains

The simplex graph $\kappa(G)$ of an undirected graph G is itself a graph, with one node for each clique (a set of mutually adjacent vertices) in G. As all of our simplexes are independent, $\kappa_j \mid j \subseteq t-1$ for tier t is formed as a disjoint subset of simplexes in $t-1$. We define κ as a mapping from an undirected graph G to a new graph $\kappa(G)$ who's vertices are cliques and compositions of cliques of G

$$\kappa : \sigma_j \to \sigma_k \mid j \subset t-1, \sigma_k \in R_{t-1}.simplices \tag{11}$$

Chain fibering is the formation of consensus blocks out of consensus blocks instead of transactions. This is varifiably sound up to isomorphism. We formulate notion of chain fibers by defining consensus in terms of a simplex graph κ. A chain fiber is given by

$$f \circ \kappa_j^k : \sigma_k \to Block_k \tag{12}$$

where κ_j^k is a simplex graph made up of chain fibers $Block_j$ in a preceding tier. The chain fibers from the preceding tier, $Block_j$, become the domain of the consensus function for tier k. We can say equivalently

$$c_k : \{Block \dots Block\}_j \to Block_k \tag{13}$$

We can formally define the mempool mem of simplex σ_k in tier t as

$$mem_k \equiv \{Block \dots Block\}_j \mid j \subset R_{t-1}.simplices \tag{14}$$

2.4 Block Sheaves

[12] Equivalence is given by pertubation.

The application of the hylomorphic recursion scheme forms a chain complex and use its dualistic construction with the metamorphic recursion scheme to create a probability space space in terms of f-co/algebras.

As our chain complex is defined in terms of homotopy types, we can use our f-co/algebras and the fact that we can crate a "combinatorial space", in order to define cohomology probabalistically. This allows us to analyze the robustness of cryptographic schemes using statistical model checking.

[11] R. Grahm Remark33

[12] [13]

[14][15] From the beginning we have assumed homotopy equivalence, thus it follows up to isomorphism that if one Radial is a topological space, so is R_K

$$\exists R \in R_K \mid R \cong T \implies \forall R \in R_K, R \cong T \tag{15}$$

where T is a topological space. Since we know by definition that R is a functor over the category of topological spaces (via definition as a topological monad) it follows that R_K constructs a chain complex under type equivalence[16].

2.5 Stitching Topological Spaces

Cohomology is obtained if we reverse the arrows in a C_R. We are concerned Cohomology because we do not have the notion of a tensor product in the homology theory of homotopy types. However the cohomology of a wedge product between two spaces is isomorphic to the product of the cohomologies. [17]

$$H_n(X \wedge Y) \cong H_n(X) \times H_n(Y) \tag{16}$$

$\otimes$ The product is a manifold from the wedge of spaces with isomorphic cohomology groups, which is enforced by homotopy type equivalence (TODO add proof, easy). As our metamorpism is a bialgebra it follows that a vector space can be formed[18]. Naturally, we can create an inner product space of a homomorphic chain complex as follows

$$H_n(X \wedge X) \cong H_n(X) \times H_n(X) = \langle X, X^* \rangle \tag{17}$$

This vector space can be formally defined in terms of the hyperplanes between Radials (show, this is key), and furthermore referred to as "hylomorphic space". A hylomorphic space $H_n(X) \times H_n(X)$ is essentially an inner product space from which we can define a probability. It can be shown that a mixture of validation protocols can be formally defined in terms of the hylomorphic space.

2.6 Infinite scalability with homomorphic parachains

We show that the criteria for cross-chain liquidity allows us to recursively define an unbouded chain complex within the homology theory of homotopy types.

Our definition of the hylomorphic space implicitly showed that R_K is a homology class within the homology theory of Homotopy types[19]. It follows that R_K forms a chain complex with homomorphism defined

[14] `https://www.seas.upenn.edu/~jean/sheaves-cohomology.pdf`
[15] `https://arxiv.org/pdf/1303.3255.pdf`
[16]
[17] R. Cavallo, Theorem 4.6 https://www.cs.cmu.edu/ rwh/theses/cavallo.pdf
[18] http://www.cs.ox.ac.uk/jeremy.gibbons/publications/metamorphisms-scp.pdf
[19] https://arxiv.org/pdf/1706.01540.pdf

as type equivalence. A homology theory of K_i types, where $H_n(-)$ is a functor [20], is given by

$$H_n(X) = ||colim_i(X_i, \theta_i)||_0 \tag{18}$$

It follows from our algebraic definition of a hylomorphism that we can construct a homology

$$H_n^h(X) = ||colim_i(F_i, h_i)||_0 \mid h_i : A \to B = g \circ f \tag{19}$$

where h is a hylomorphism.

It follows that R_K is isomorphic to H_n^h. Proof: show through our definition of R as a monad that R is a functor over the category of simplexes and that hylomorphism between Radials preserves type homotopy through type equivalence.[21]

By definition C_K is unbounded which implies that the chain complex is unbounded and our network bandwidth follows the following exponential formula:

$$\begin{aligned} f(x,n) &\cong \alpha x \mod_n \\ U(f,x,t) &= (cf(x,n)^t \end{aligned} \tag{20}$$

where c, α, n are scaling params. TODO, tie these together in our definition of Radial.

3 Conclusion and Applications

https://golem.ph.utexas.edu/category/2012/09/general$_c ovariance_i n_h omotopy.html$

Information geometry is the holy grail of ml. But we can't build models that fine tuned because of junk data. The free flowing wellspring of factual data points will allow for the masses to compete with uber and google in a maketplace of ml apps. Tying everything back to our original simple type theoretic definition, if we have a universal type systems for blockcahins, enforced by compiler pugins for all languages, we get two major benefits. One is compile time checks of cross chain liquidity and the second is the ability to use functional programming techniques to implement blockchain protocols. As an example, we can show that consensus is actually just a flatmap over a a monad of defined as a cluster of nodes acting as the carrier for distributed consensus.

`https://homepages.inf.ed.ac.uk/rsarkar/papers/hyperbolic.pdf`

Introduction

[20] R. Grahm Theorem 34 https://arxiv.org/pdf/1706.01540.pdf

[21] ensure above definition satisfies criteria from R. Grahm