Hylochain and Blockchain Cohomology

Wyatt Meldman-Floch

February 17 2018

Abstract

We introduce Hylochain a DAG of blockchains. We show that a Hylochain is a chain complex within the homology theory of homotopy types. We propose the term Chain Complex to describe this class of cross chain distributed ledger technology.

Introduction

Blockchains can be defined generically in terms of a monoid, a functor and a sheaf. Our monoid is an execution context within which consensus is performed. The functor is consensus and our sheaf is our block.

Fundamental Data Structures and Types

Tier <: Numeric

Numeric type that is used to define ordering among the Radial monoid (see below)

BlockData[Tier] <: U

Consider a type *BlockData* which serves as the parent type (under universal type U) of all data going on chain. All BlockData is equivalent via covariance and thus all BlockData can be compressed into a Block.

Block[U] <: U

Contains compressed form of Block Data. This is the result of consensus. It is worth noting that $Block[U] \equiv Block[BlockData[Tier]]$ through covariance. Block[U] is a Fix Point Type [1]

Transaction <: BlockData[0]

Transaction is a subtype of BlockData that can only exist on the bottom tier. It is the building block of our currency.

Definition: Consensus Simplex, σ

A set of validators, which undergo cryptographic consensus to produce a *Block*. Formally defined as a Simplex.

$$\sigma \cong collection[node] \tag{1}$$

Node ADT

Let n be an abstract data type Node, with three attributes, a *protocol* process a *consensus* process and a *chain* class. Formally we define n as the algebraic data type

```
/*
should define algebraically eventually
*/
case object Node {
  val chain: Chain = new Chain()
  val protocol: => Seq[BlockData[T]] = new Protocol()
  val consensus: => Block[U] = new Consensus()
}
```

Network Topology

The network topology of a hylochain is a clique complex, and is formally defined as an ordered set of functors over the category of simplexes, R_K of Radials R_t

[1] https://jto.github.io/articles/typelevel-fix/

ordered by Tier $t \in T$

$$R_K : \{R_0 \dots R_T\} \tag{2}$$

Simplex

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 simplex iff:

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

$$\forall n \in \sigma, \exists e \in E \mid e \equiv \sigma \setminus \{n\} \tag{3}$$

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:

$$\forall n \in \sigma_k, st_K(n) \equiv \sigma_K \tag{4}$$

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

$$\exists g : \sigma \to d, \mid d \subseteq \sigma \tag{5}$$

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

$$SC(\sigma_k) = \bigcup_k st(n) \in I_G \ \forall k \in K \tag{6}$$

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

$$\begin{aligned} SC(\sigma_k) &= \bigcup_k st(n) \\ &\equiv st(n) \ \forall n \in k \end{aligned} \tag{7}$$

[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

Radials: Tiered Hypergraphs

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

```
case class Sigma(nodes: Node*)

trait Radial[T <: Tier] {
/*
simplex and starCluster are hyperedges
*/
   val starCluster: Sigma[T-1]
   val simplices: Sigma[T]* \\ note this is variadic
   def hyperPlane[T1, T2]: Sigma[T1] => Sigma[T2]
}
```

The hypergraph for all simplexes σ_k within Tier t is given by the two element set

$$H_{t,k} = \{I_{g_{t-1}} \mid g_{t-1} \subset G_{t-1}, \sigma_k\} \tag{8}$$

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, but of transactions which are isomorphic to all subtypes of BlockData via covariance.

Blockchain Topology

We define the primitives of our DAG chain. We come to the conclusion that our DAG chain is a directed acyclic graph who's direction is given by simplex graph[9] κ and topological ordering follows the tiered ordering of R_K. The simplex graph $\kappa(G)$ of an undirected graph G is itself a graph, with one node for each clique (a

[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
[9] wikipedia/Simplexgraph

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

$$\kappa : \sigma_j \to \sigma_k \mid j \subset t-1, \sigma_k \in R_{t-1}.simplices \tag{9}$$

Chain Fibering

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

$$f \circ \kappa_j^k : \sigma_k \to Block_k \tag{10}$$

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

$$c_k : \{Block \dots Block\}_j \to Block_k \tag{11}$$

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

$$mem_k \equiv \{Block \dots Block\}_j \mid j \subset R_{t-1}.simplices \tag{12}$$

Chain Complexes and Polymorphic Validation

There is a namely notion in topology, the chain complex, which accurately describes the our network topology in relation to blockchain topology. We propose the definition of a Chain Complex, as a collection of blockchains that are connected, composed or scaled through chain fibering and/or parachains. We define chain fibers and parachains in terms of homological algebra over chain complexes and show how to "stich" these chains together through type equivalent validation protocols.

Validation is the cornerstone to blockchain technology. We show how to formulate a probability space upon which we can define and implement a probabilistic consensus mechanism.

First we define the space of hyperplanes between Radials and show that this is a metric space. Every metric space is also a topological space, so it serves us

to first define R_K as a topological space. It is trivial to show that $n \in k\forall K$, σ, Radial.*simplices* satisfied the necessary axioms[10] of a topological space and just as trivial to extend this to the union of simplices across Radials. We leave this as an exercise for the reader.

The topological space we are interested in is actually a mixture of $n \in k\forall K$, $\sigma_k \in K$ and $R \in R_K$. Because σ_k is an independence complex for all $k \in K$, we need to use the concept of homotopy to "stitch" these topologies together. We show that the Hylomorphism recursion scheme and it's parameterization via bialgebra allow us to "stitch" these topologies together under homotopy defined by typesafety.

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

$$\exists R \in R_K \mid R \cong T \implies \forall R \in R_K, R \cong T \tag{13}$$

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[11].

$$C_R = R_0 \xrightarrow{h_0} R_1 \dots R_{n-1} \xrightarrow{h_{n-1}} R_n \tag{14}$$

where h_0 is a hylomorphism.

A hylomorphism can be defined in terms of algebras and coalgebras:

```
def hylo[F[_] : Functor, A, B](f: F[B] => B)(g: A => F[A]): A => B =
  a => f(g(a) map hylo(f)(g))
```

Where g is an f-coalgebra and f is an f-algebra [12]. It is trivial to note that process of distributed consensus is isomorphic to a hylomorphism.

Hylomorphic Vector Space

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. [13]

[10] http://mathworld.wolfram.com/TopologicalSpace.html

[11]

[12] http://free.cofree.io/2017/11/13/recursion/

[13] R. Cavallo, Theorem 4.6 https://www.cs.cmu.edu/ rwh/theses/cavallo.pdf

$$H_n(X \wedge Y) \cong H_n(X) \times H_n(Y) \tag{15}$$

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[14]. Naturally, we can create an inner product space of a homomorphic chain complex as follows

$$H_n(X \wedge X) \cong H_n(X) \times H_n(X) = \langle X, X^* \rangle \tag{16}$$

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.

Infinite scalability through 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[15]. It follows that R_K forms a chain complex with homomorphism defined as type equivalence. A homology theory of K_i types, where $H_n(-)$ is a functor [16], is given by

$$H_n(X) = ||colim_i(X_i, \theta_i)||_0 \tag{17}$$

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

$$H_n^h(X) = ||colim_i(F_i, h_i)||_0 \mid h_i : A \to B = g \circ f \tag{18}$$

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.[17]

[14] http://www.cs.ox.ac.uk/jeremy.gibbons/publications/metamorphisms-scp.pdf
[15] https://arxiv.org/pdf/1706.01540.pdf
[16] R. Grahm Theorem 34 https://arxiv.org/pdf/1706.01540.pdf
[17] ensure above definition satisfies criteria from R. Grahm

Typesafe Cross-chain Atomic Swaps

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 [18] (we can easily show with cw-complex, should add diagram)

$$f_i \circ \phi_i = \theta_i \circ f_{i+1} = \theta_i \circ f_i = \theta_i \circ \phi_i \tag{19}$$

A tensor defines chain mappings[19] 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 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[20] 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.

Scaling through Recursive Parachains

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

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

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

[20] R. Grahm Remark33

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

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

Conclusion

We have described Hylochain and the basic notion of a Chain Complex. We are inspired by the possibility of applying sheaf theory to construct vector fields out of Blocks[21][22] for a wide range of applications.

[21] https://www.seas.upenn.edu/ jean/sheaves-cohomology.pdf
[22] https://arxiv.org/pdf/1303.3255.pdf