# Topological Characterisation of Trust in Consensus Networks

**Jeffrey Morais**$^{a,b}$, **Peter P. Rohde**$^{b,c,d}$, **Igor Boettcher**$^{e,f}$

$^{a}$*Department of Physics and Astronomy, University of Victoria, Victoria, BC V8W 3P6, Canada*
$^{b}$*BTQ Technologies, 16-104 555 Burrard Street, Vancouver BC, V7X 1M8 Canada*
$^{c}$*Centre for Quantum Software & Information [UTS:QSI], University of Technology Sydney*
$^{d}$*Hearne Institute for Theoretical Physics, Department of Physics & Astronomy, Louisiana State University, Baton Rouge LA, United States*
$^{e}$*Department of Physics, University of Alberta, Edmonton, Alberta T6G 2E1, Canada*
$^{f}$*Theoretical Physics Institute, University of Alberta, Edmonton, Alberta T6G 2E1, Canada*

*E-mail:* jeffrey.morais@mail.mcgill.ca, dr.rohde@gmail.com, iboettch@ualberta.ca

Abstract: Consensus protocols in blockchain transactions suffer from scaling issues when adopting proof-of-work schemes. These schemes rely on parties competing to solve cryptographic puzzles for stakes in transactions and are inefficient due to an artificial reduction in their transaction rate when scaling up networks [to prevent inflation and multiple winners]. Instead, we adopt *proof-of-consensus* schemes whereby autonomous networks of known parties are quantum randomly allocated into sub-networks to perform consensus on independent transactions. Such networks have their compliance tested during consensus and so are known as *consensus networks*. These schemes do not require stakes in transactions as they instead rely on mutual benefit and do not run into the scaling inefficiencies of proof-of-work schemes. The security of such a protocol is characterized by the *trust* between parties in the network [and additionally external clients], a dynamic quantity that changes over time. We present a *topological* formulation of the dynamics of trust in closed consensus networks to describe how they evolve in time in an efficient and generally covariant manner. We compute the intersection of trust between parties in a network, and the trust as viewed by clients, to define an overall effective trusted network to be offered as a service. Finally, with the use of algebraic topology and surgery theory, we present a combinatoric way for networks to autonomously split off and combine with each other for a natural way to scale up the amount of transactions verified, for more efficiency overall.

## Contents

## 1 Introduction

Consider a collection of parties which form a set known as a *network*, where its constituents elements are referred to as a *nodes*. Much like an ensemble of particles, these nodes can interact with one another such as participating in *transactions*. The network may be affected by external sources such as through centralized arbiters that oversee said transactions impartially and securely. In nature we find that transactions between parties are usually arbitrated by banks which can take a cut of the transaction as a service fee. Naturally then, it would be beneficial for the nodes to minimize the degrees of freedom between themselves and so remove the intermediate middle man taking the form of a centralized authority; the bank. These independent transactions, however, are subject to parties *colluding* with one another to rig transactions between nodes without central oversight. Thus, we would like a decentralized system to process transactions between nodes in a network of parties with ample security to avoid unlawful manipulation. Herein lies the concept of blockchains.

A *blockchain* is an immutable data structure whose information is stored non-locally across the network, where each element of the blockchain — known as a *block* — contains the data of a transaction event. For the purposes of security, this data is encrypted via a function whose inverse is computationally infeasible to compute [known as a *hash*], and each block contains information of the previous block in the chain. The combination of the hash and information being stored in subsequent blocks prevent the transaction block from being manipulated. By construction, the blockchain is immutable: once an additional block is added to the chain, its information is fixed and cannot be altered. Now, one would wonder how to control the legitimacy of transactions when populating the blockchain if there are no central arbiters. This would have to be some form on *consensus* between the nodes of the network in which an agreement is made on the validity of the transaction and the order in which it is added to the blockchain. For methods in consensus, one could consider either open or closed networks. An *open* network is one in which external nodes can join the network freely to participate in consensus events to agree on the validity of transactions. This structure is more susceptible to colluding amongst nodes as an arbitrary amount of malicious/corrupt nodes can join to skew the consensus in their favour. This problem is attenuated in closed networks given a fixed amount of known nodes. For the more popular case of open networks, the usual consensus algorithm is known as a *proof-of-work* scheme. Given a transaction event which contains a hash [for which it is computationally infeasible to solve for its inverse], à la style of brute force nodes compete to figure out the hash's input via sampling a random distribution of inputs. Randomly sampling a inputs is extremely inefficient and so this process does not fall into the *complexity* class **P**, a class of problems that can be quickly solved in polynomial orders of time. Once a node randomly stumbles upon the correct input and shares it with the rest of the network, the transaction can be quickly verified by the other nodes. Thus a proof-of-work scheme for verification belongs instead to the complexity class **NP**, a class of problems of which could be verified quickly in polynomial time. Once verified and thus consensus has been made, the node which found the initial input is rewarded with a portion of the transaction, and a block is added to the blockchain. Problems present themselves when attempting to have scalable proof-of-work schemes such as egregious energy costs per transaction which are many orders of magnitude higher than one arbitrated by a bank. Furthermore another problem is the artificial reduction in transaction rates to prevent degeneracies in the pool of winners and prevent inflation of the underlying currency.

*What if we make use of quantum computers to compute these inputs and rid of these inefficiencies?* While classically the amount of inputs used to solve the hash problem is of the order $\mathcal{O}(N)$ — where $N$ is the size of the domain of the hash function — quantum algorithms can solve the problem more quickly given that they only need $\mathcal{O}(\sqrt{N})$ inputs. Why not then make use of quantum computers for consensus in networks one might ask, given a quadratic speedup? The problem with using quantum computers for solving unstructured problems with inverting [injective] functions is that it violates *progress-free* condition. This means that nodes that have solved previous block puzzles would have an advantage over ones that have just joined to solve the current hash input. What we *can* do to make use of the advantage that quantum algorithms holds over classical computations is by *sampling.* Recall that the use of quantum mechanics is that one can store information non-locally through entanglement for which there is associated uncertainty. This presents quite the incentive to save on computational demand as one would not need to collapse the state until measurement and so working with a state in superposition [which contains all possible information of the system] is more efficient. This of course, comes with its own share of problems with scalability as the uncertainty increases further and the need for quantum error correction and fault-tolerant codes come into play. Unlike a decision problem in which a precise solution is given [the hash input], with sampling you take measurements from a large superposition and converge to the solution given some estimated probability. One for instance could make use of *boson-sampling*, a consensus algorithm that estimates [via convergence] the expectation value of matrix permanents for boson scattering events. This could be implemented as a proof-of-work scheme for networks verifying the validity of a transaction when populating a blockchain.

Now, boson-sampling falls into its own complexity class **BosonSampP** and is thought to be strictly contained within the class of sampling problems that can be efficiently solved on a quantum computer, **SampBQP** [1]. Although these problems are sampled more efficiently with a quantum framework over that of a classical one, the fact still remains that open networks are vulnerable to external manipulation of consensus outcomes, and proof-of-work schemes are exceedingly unscalable. It is for these reasons we instead consider an alternate consensus scheme which makes use of closed networks. A *closed* network is one in which the amount of nodes [and the fraction of which are malicious] is fixed. For the purposes of consensus, we would like a scheme that is highly resistant to malicious nodes colluding to manipulate the outcome of consensus by forcing an unlawful majority. In this endeavour we could prevent this by splitting these malicious nodes into subsets and taking local consensus from these sets. To the maximal degree, the allocation of these subsets must be *quantum random* as to disperse these malicious parties among honest ones and suppress their strategy. Such a scheme is known as a *proof-of-consensus* scheme. If a subset of the network forms consensus and it reflects the will of the majority, the colluding minority will fail. In order to do so we test the compliance of nodes in sub-networks which reflects the amount of trust nodes have in each other. Networks which are quantum randomly assigned to sub-networks for consensus and whose compliance is tested are known as *consensus networks.* Unlike proof-of-work schemes, no stake in a transaction must be lost as the scheme instead relies on mutual benefit: for every transaction a node requests to be verified, so too must they participate in an equal amount of transaction verification. Furthermore, proof-of-consensus schemes do not run into the scalability issues and high energy costs of proof-of-work schemes. To characterize the security of such a protocol, we will need to mathematically describe the trust between nodes with a consensus network over time. Taking inspiration from the non-local aspects of quantum theory, for efficiency we will want to make use of a *global theory* [unlike a theory in which nodes share local information about transactions]. For global theory one can employ *topology*[†] which captures the global aspects of a space [in our case the space of networks] in a manner that does not depend on local aspects such as geometry. The use of topology moreover also allows us to have a generally covariant theory [a theory which is invariant under diffeomorphisms or deformations of the space] which allows us to characterize information through topological

[†] *Differential topology* characterizes the properties of structures on manifolds that have only trivial local *moduli* [parameter spaces that are typically orbifolds] while *differential geometry* studies structures that have non-trivial local moduli. Points in moduli space correspond to solutions of geometric problems which are identified if isomorphic. An example of a moduli space would be the space of all Ricci flat metrics on a Calabi-Yau manifold [described by a vanishing second Chern class $c_2$].

invariants. In this paper we prescribe a topological characterization of trust [and hence security] in consensus networks used in proof-of-consensus schemes for efficient transaction verification. First we motivate the construction for topological consensus networks how how breaches in trust create bifurcations in the form of cobordisms. We then describe how independent networks can combine with each other based on trust given by topological invariants. Then we look at the presenting this framework as a service to clients through the intersection of trust between the client and the network, and the network with itself. Finally, we come up with a protocol for autonomous networks to evaluate others and combine with a topological classification of networks [and their associated history]. This gives us a natural way to scale up networks for a more efficient service of verification without running into the inefficiencies as suffered by proof-of-work schemes.

## 2 Topological consensus networks

Here we outline the topological characterization of consensus networks. First we look at how a topological consensus network — described as a manifold — can bifurcate into different sub-networks via compliance [trust] checks at the end of consensus events. We demonstrate the different ways they may evolve in time with the use of cobordisms to represent their temporal history. With the use of topological invariants — such as those arising in knot theory — we characterize a class of consensus network histories to determine how networks may autonomously combine with other networks based on criteria set by the network and clients. Finally, we demonstrate how the intersection of trust shared by the network and client can be used as a service.

### 2.1 Breaches in trust as cobordisms

Let's begin with the construction of a topological consensus network. A *regular* consensus network — whose elements are referred to as *nodes* — is a closed 1D set of parties wanting to have their decentralized transactions approved. To do so, for each transaction a node requests to be verified, so too must they participate in an equal amount of consensus rounds of transaction verifications. To use a *topological* theory, we require more dimensions. This is due to 1D having relatively trivial topology, with all loops in it contracting to a single point without encountering discontinuities. This comes from a 1D theory lacking *voids*[†] which are higher dimensional empty sets which cause the space to have non-zero genus [roughly speaking the number of holes]. For a 2D theory we will consider a space which contains the information of all possible nodes and transactions, and define it as the product space:

$$\mathcal{Y} \equiv \mathcal{N} \times \mathcal{T}, \tag{2.1}$$

where $\mathcal{N}$ is the set of all possible nodes and $\mathcal{T}$ is the set of all possible transactions. We refer to $\mathcal{Y}$ — the space of all nodes and transactions — as the *ambient* space. Being

[†] For some space $\mathcal{M}$ with $\dim \mathcal{M} > 1$, we can consider the Betti number $b_2 = \dim H^2(\mathcal{M})$ where $H^2(\mathcal{M})$ is the second cohomology group over $\mathcal{M}$. It tells us which 2-forms exist in the cotangent space over $\mathcal{M}$ as well as how many voids [or cavities] there are.

that the information of the nodes and their transactions are independent [and discrete] from one another we could just take $(\mathcal{N}, \mathcal{T}) = (\mathbb{Z}, \mathbb{Z})$ thus $\mathcal{Y} = \mathbb{Z}^2$. However, we will utilize the framework of a *continuous* theory [to define the notion of continuous functionals and operators] by taking the continuum limit and replacing the sets to $(\mathcal{N}, \mathcal{T}) = (\mathbb{R}, \mathbb{R})$ and so we instead have $\mathcal{Y} = \mathbb{R}^2$. To have a *topological* space, we require that the set $\mathcal{Y}$ and the collection of its *open* subsets satisfy the conditions [2]:

i) $\mathcal{Y}$ and its empty subset are open,

ii) If subsets $(\mathcal{Y}_a, \mathcal{Y}_b) \subseteq \mathcal{Y}$ are open, this implies the intersection $\mathcal{Y}_a \cap \mathcal{Y}_b$ is also open,

iii) If subsets $\mathcal{Y}_a \subseteq \mathcal{Y}$ are open, this means the union space $\bigcup\limits_a \mathcal{Y}_a$ is also open.

The open subsets $\mathcal{Y}_a$ form the *topology* of $\mathcal{Y}$ and cover the entire topological space. On each of these subsets we define a *chart* to be a continuous map $\varphi_a : \mathcal{Y}_a \to \mathbb{R}^2$. These charts allow us to work in locally flat coordinates [whereby the connection on the space of 2-forms, $\Lambda^2\mathcal{Y}$, vanishes]. Finally, to be a *topological manifold*, for any two charts $(\varphi_a, \varphi_b)$ on $\mathcal{Y}$, the *transition function* which is written as the composition $\varphi_a \circ \varphi_b^{-1}$ must be smooth [integrable] over $\mathcal{Y}$. We thus define a **topological consensus network** $\mathcal{G}$ as a submanifold of the product space $\mathcal{Y}$ that is closed, meaning it contains it's boundary [for $\mathcal{G} \subseteq \mathcal{Y}$ and $\dim \partial\mathcal{G} = \dim \mathcal{Y} - 1$, then $\partial\mathcal{G} \neq \emptyset$].

Now, one could imagine how such networks can evolve over time. We can capture this information succinctly with the use of *Lorentzian*[†] manifolds such as that of spacetime in general relativity. If $\mathcal{Y}$ contains all possible information of the network's nodes and transactions, we can consider all possible evolutions of the network through the inclusion of an extra temporal dimension which we take to be simply $\mathbb{R}$. The inclusion of time is done through a Cartesian product and thus we define our **networktime** as the following product manifold:

$$\mathcal{M} = \mathbb{R} \times \mathcal{Y}. \tag{2.2}$$

Here $\mathbb{R}$ is the real line giving us a natural parametrization for time, and $\mathcal{Y}$ is a 2D manifolds describing the space of topological consensus networks. By this construction $\mathcal{M}$ is the space of all possible topological consensus network outcomes. *What does an evolution of a topological consensus network $\mathcal{G}$ in $\mathcal{M}$ look like?* Consider some topological consensus network $\mathcal{G} \subseteq \mathcal{Y}$ which is invariant under time translations [does not evolve in time]. Such an evolution would trivially trace out the following manifold in $\mathcal{M}$ as:

[†] [Pseudo-Riemannian] manifolds with a metric signature of $(1, n-1)$, meaning its eigenvalues signs are given by a list $(-, +, \ldots, +)$. Such is the case for the *Minkowski* space metric $\eta_{\mu\nu} = \mathrm{diag}(-1, +1, +1, +1)$ in general relativity when $D = 4$. The first eigenvalue corresponds to the time dimension, and due to the negative sign, measuring distances in Minkowski space depends on the following line element:

$$ds^2 = \eta_{ab} dx^a \otimes dx^b = -dt^2 + dx^2 + dy^2 + dz^2.$$

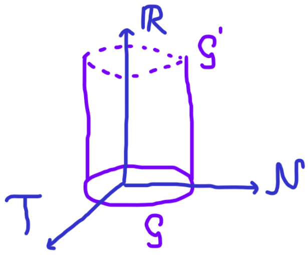

**Figure 1**. Evolution of a static topological consensus network $\mathcal{G}$ in the ambient networktime space $\mathcal{M} = \mathbb{R} \times (\mathcal{N} \times \mathcal{T})$. The network evolves trivially to the same network $\mathcal{G}'$ some time later and traces out a cylindrical manifold in networktime $\mathcal{M}$.

At first glance time evolution appears to be specified through boundary conditions on the network along the time dimension, separated by some time interval $\mathcal{I} \subset \mathbb{R}$. The manifold traced out can be described via the product $\mathcal{H} = \mathcal{G} \times \mathcal{I} \subset \mathcal{M}$. Here $\mathcal{H}$ is the **network history** which captures all information of the network over time. It is utilizing these histories which will allow us to determine compatibility of independent networks to autonomously combine. A subtlety must be noted which is that there is a *degeneracy* in the history of a network for a given identical boundary condition; the same conditions can apply to different evolutions of a network. Consider two cases: one in which the initial and boundary condition is specified to be a single network, and one in which only the boundary condition is specified to be a single network. For these two cases we have the following scenarios:

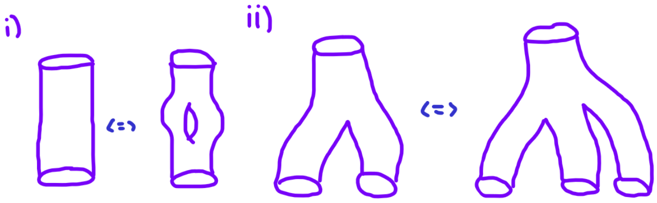

**Figure 2**. Visualization of boundary condition degeneracy. On the left subfigure we see specifying the same initial and boundary conditions can admit multiple unique histories and so there is a *degeneracy* [or multiplicity]. On the right subfigure we see that only specifying the boundary condition can have multiple histories satisfying that condition, again implying degeneracy.

While the second subfigure demonstrates the equivalence of histories of different topological consensus networks combining to form a single network [for different amounts of initial networks], the first subfigure is a bit strange; one of the histories has non-trivial genus[†]. How do we interpret this? The history admitting a void can be decomposed as the following:

[†] Formally, the genus of a surface [with no punctures] is the maximum number of non-self-intersecting closed curves that you can draw on a surface without disconnecting it. While a torus has a unity genus, a pair of pants for example has vanishing genus.

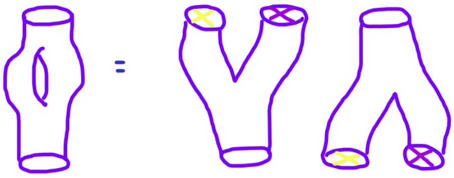

**Figure 3**. Decomposition of a topological consensus network history with non-trivial genus. Here we have split it into two other histories and identified different points on the boundaries. The splitting of a manifold this way is known as a surgery [in surgery theory], whereas combining the manifolds is known as gluing. More on this later.

There are two ways to interpret this decomposition. On one hand the network starts as a whole, goes through a round of consensus and bifurcates into two networks due to suspected malicious nodes. Then after another round of consensus where the malicious nature is proven to be minimal, it recombines into a single network. The other way of viewing this decomposition is combining one network history with another, i.e., a method in which networks can combine to form larger networks for more efficient communication and verification of transactions.

The degeneracy as noted before — either coming from specifying one or both conditions — means that to describe a network history, it isn't enough simply to specify both the initial and final conditions. One must also take into account the information between these conditions, and to do so we will make use of cobordisms[†] and surgery theory. To do so we first review equivalence relations and classes. An *equivalence class* is a set where all the elements are equivalent to each other in some way. Given a set $X$ and some element $a \in X$, the equivalence class of $a$ in $X$ is given by:

$$[a] = \{x \in X : x \sim a\}. \tag{2.3}$$

Here $\sim$ is the *equivalence relation* which tells us how two elements are equivalent [the most common equivalence relation is the equal symbol: $=$]. Thus, the class $[a]$ is the set of elements of $X$ that are equivalent to $a$, and is known as a *partition* of $X$. The set of all equivalence classes or partitions of $X$ is known as the *quotient set*, which is defined as:

$$X/\sim = \{[x] : x \in X\}. \tag{2.4}$$

The quotient set is usually defined between two sets, such as $X/Y$ for some other set $Y$. This specifies the equivalence relation where two elements of a partition of $X$ are equivalent if they differ by an element of $Y$. We will see that the specification to uniquely define a network history comes from a combinatoric series of possible network interactions. Now, a *cobordism* is equivalence relation on the class of compact manifolds of the same

[†] Cobordisms are used to describe wormholes and entangled particle creation in *topological quantum field theories*. In such theories, one considers a category in which the *objects* are compact $n$-dimensional manifolds and the *morphisms* [the maps between the objects] are cobordisms. Topological defects on these objects are interpreted as particles, and in this sense we can understand particle interaction through different mappings of the category's objects.

dimension, and can be interpreted as a set of instructions for a manifold $M$ to evolve over time into another manifold $N$ in such a way that their own boundaries are preserved [3]. Put more precisely, an $(n+1)$-dimensional cobordism is a quintuple of information:

$$(W; M, N, i, j), \tag{2.5}$$

where $W$ is an $(n+1)$-dimensional compact manifold with a boundary $[\partial W]$, $(M, N)$ are compact $n$-manifolds, and $i : M \hookrightarrow \partial W$ and $j : N \hookrightarrow \partial W$ are embeddings [structure contained within another instance, such as a subgroup within a group] of the manifolds to the boundary of $W$. The embeddings have disjoint images which adhere to the union condition $i(M) \sqcup j(N) = \partial W$. We can visualize this cobordism via the following figure:

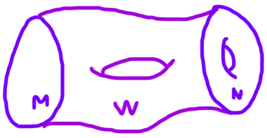

**Figure 4**. Cobordism between two compact manifolds $(M, N)$ via an intermediary manifold $W$. Here the boundary of $W$ is the disjoint union of $M$ and $N$, given as $\partial W = M \sqcup N$. Here we have dropped the embedding maps as it is implied the compact manifolds $(M, N)$ are contained within the *closure* of the higher dimensional manifold $W$.

Two manifolds $(M, N)$ are called *cobordant* if such a cobordism exists and they share topological properties such as Chern/Pontryagin numbers [4]. From this we can construct *cobordism classes* which consist of all manifolds that are cobordant to a fixed manifold. In this sense we can fix the initial compact manifold [our topological consensus network] and consider the cobordism class of all manifolds which it is cobordant to, meaning all possible outcomes of the evolution of the network. More explicitly, two cobordisms of networks in this class are considered equivalent if they can be continuously deformed into each other. Thus, cobordisms give us a prescription on how to characterize network bifurcation based on *trust* evolving overtime with each round of consensus [and subsequent compliance checks]. The cobordism manifolds correspond precisely to the *history* $\mathcal{H}$ of a topological network $\mathcal{G}$ and hence how it evolves in time.

Now for some intuitions on cobordisms [of topological consensus networks], let us consider a few examples. The most trivial example of a cobordism is the 1D cobordism between 0D manifolds $M = \{0\}$ and $N = \{1\}$, which is given by the unit interval $W = [0, 1]$. Another fairly simple example would in in Fig. 3 where the first piece of the decomposition represents a cobordism between some initial topological consensus network $\mathcal{G}$ and two temporary networks. Finally, consider a cobordism from a 2-disk $D^2$ [filled in unit circle $S^1$] to a modified 2-disk $Y$ with a handle $H$ attached [3]. We can write such a cobordism as a mapping $\alpha : D^2 \Rightarrow Y \circ H$ and visualize it as the following:

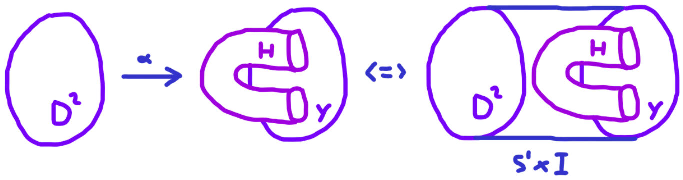

**Figure 5**. Cobordism between a disk and a modified disk with a handle. Here we characterize the length of the boundary of the cobordism [the distance between the cobordant manifolds] by some interval $I$ and so write the boundary as $\partial W = S^1 \times I = D^2 \sqcup Y \circ H$.

Thus we can interpret the [categorical][†] cobordism as a continuous mapping between compact manifolds whose boundary is given by a higher dimensional ambient manifold. This is a direct result of the relative **trust** of nodes in a given network and is why the topological network can bifurcate into sub-networks in the first place. Thus, we will use cobordisms as the language to describe the evolution of a topological consensus network, which is succinctly captured by the network history in networktime. In the following section we will describe how different cobordisms [and hence network histories] maybe be combined via surgeries in a combinatoric sense, analogous to particle interactions in quantum field theory.

## 2.2 Composite consensus networks

Now that we have a prescription for how topological consensus networks bifurcate into sub-networks due to breaches in trust [via cobordisms], we discuss how separate networks can *interact* with each other. An equivalent statement would be how independent network histories can *combine* into composite networks. Recall that boundary conditions alone are not enough to specify a unique network evolution and so we require additional information. We characterize this missing information as the interaction of different network histories [cobordisms] via a series of possible network interactions.

First, we will make use of *surgery theory* to make sense of stitching together different networks which have evolved independently in time. The purpose of such a theory is to produce a finite dimensional manifold from one or many others in a well-defined manner. A *surgery* refers to cutting out parts of a manifold and replacing it with a part of another manifold in such a way that its topological invariants are preserved. The cut is matched up along open boundary subsets of the manifolds [given the existence of a diffeomorphism $\phi$ between them]. Morse theory tells us that a manifold can be obtained from a surgery by a sequence of spherical modifications if and only if the manifolds belong to the same

[†] Here $\alpha$ in in fact a 2-morphism in a 2-category. This cobordism can be understood as a pair creation of particles in a topological quantum field theory. Being that $D^2$ and $Y \circ H$ can be viewed as cobordisms from the empty set to the unit circle $S^1$, we can capture the cobordism in the figure via the following categorical diagram [3]:

$$\begin{tikzcd}
\emptyset \arrow[r, bend left=50, "Y\circ H"] \arrow[r, bend right=50, "D^2"'] \arrow[r, phantom, "\Uparrow \alpha"] & S^1
\end{tikzcd}$$

cobordism [equivalence] class. Thus we can combine the network histories under a *gluing* surgery in which the open subsets are identified [the points on each subset must be the exact same] if the histories are in the **same** cobordism class. We present gluing surgery in the following.

Consider two manifolds $(M, N)$ with respective open subsets $(U, V)$ which we would like to glue along by identifying the points of each subset. To do so, we require the existence of the diffeomorphism $\phi : U \to V$ between subsets. We write the enlarged manifold [$M$ glued with $N$] as the space [5]:

$$M \cup_\phi N = (M \sqcup N)/\sim . \tag{2.6}$$

Here we say that the two manifolds glued together is the disjoint union of the two with an identification of open subsets [hence the modulo equivalence relation]. This is the set of all equivalence classes or partitions of $M \sqcup N$ such that two elements $u \in U$, $v \in V$ are equivalent up to the diffeomorphism $\phi$: $u \sim v = \phi(u)$. This means that the points exist on the same glued boundary. *What would this look like for network histories part of the same cobordism class?* Consider two network histories $(\mathcal{H}, \mathcal{H}')$ with respective boundaries $(\partial\mathcal{H}, \partial\mathcal{H}')$. We interpret these boundaries as a disjoint collection of initial and final topological consensus networks [that is to say, the amount of independent networks before and after time evolution]. For example, a network which splits in two will have a network history with three disjoint pieces: one initial network piece and two final network pieces. One could generally consider a network history $\mathcal{H}$ with $n$ initial networks $\{\mathcal{G}_a\}$ and $m$ output networks $\{\tilde{\mathcal{G}}_b\}$. We would write such a boundary of a the history as:

$$\partial\mathcal{H} = \bigsqcup_{a=1}^{n} \mathcal{G}_a \bigsqcup_{b=1}^{m} \tilde{\mathcal{G}}_b. \tag{2.7}$$

Thus for two network histories $(\mathcal{H}, \mathcal{H}')$ to be glued, we require the existence of diffeomorphisms that maps between the output boundaries of $\mathcal{H}$ to the input boundaries of $\mathcal{H}'$. If $\partial\mathcal{H}$ contains output boundaries $\tilde{\mathcal{G}}_a$ and $\partial\mathcal{H}'$ contains input boundaries $\mathcal{G}'_b$, then to glue the histories together we require the existence of the diffeomorphisms:

$$\phi_{ab} : \tilde{\mathcal{G}}_a \to \mathcal{G}'_b. \tag{2.8}$$

For the resulting glued space to remain a manifold, we require the graph of $\phi_{ab}$ — given by $\Gamma(\phi_{ab}) = \{(h, \phi_{ab}(h)) \mid h \in \mathcal{H}\} \subset \mathcal{H} \times \mathcal{H}'$ — to be closed in the product $\mathcal{H} \times \mathcal{H}'$. This ensures that the resulting space is Hausdorff and thus a manifold. Finally with the set of diffeomorphisms defined as $\{\phi_{ab}\} \equiv \phi$, we write down the **glued topological consensus network history** as:

$$\mathcal{H} \cup_\phi \mathcal{H}' = (\mathcal{H} \sqcup \mathcal{H}')/\sim, \tag{2.9}$$

where elements of the glued space are equivalent up to the diffeomorphisms $\phi$ [that map between the disconnected network pieces of $\mathcal{H}$ and $\mathcal{H}'$]. Now that we know how to combine network histories, we must consider how networks can *interact*. That is to say, what are the different ways networks can interact given a set of initial and boundary conditions? For this we take inspiration of the combinatorics behind particle interaction in *quantum field theory* (QFT). Consider a *scalar* quantum field theory, meaning a quantum theory that contains a scalar field representing bosons of spin 0. We encode how different bosons can interact given a vertex term $\lambda\varphi^4$ in the theory's Lagrangian $\mathcal{L}$, which looks like:

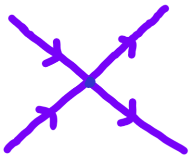

**Figure 6**. Interaction vertex of $\varphi^4$ scalar quantum field theory that allows for two incoming and outgoing particles. The vertex can be iteratively combined with other vertices to come up with potential particle evolutions through interaction.

Now given this interaction vertex we can describe particle *interactions*, otherwise known as the mechanism through which particles can fundamentally share information. All the different ways in which they share information — or *interact* — is given by all possible permutations of connecting interaction vertices. For example, can a single particle interact with itself and if so, what are all the ways it can? We visualize a spin 0 bosonic particle interacting with itself with the use of 2-point functions [expectation values of two operators $\langle\varphi\varphi\rangle$ in statistical mechanics when rotating our system to imaginary time] :

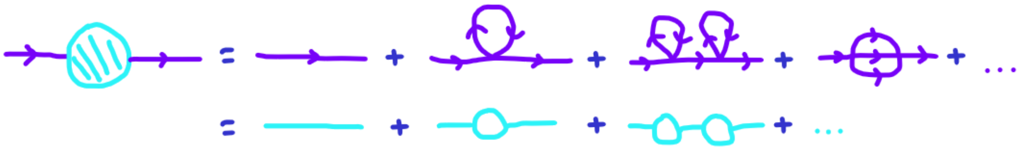

**Figure 7**. 2-point function for scalar particles. The first equality represents all possible ways a particle can come in, interact in some way, and then outcome as a single particle. The amplitude of a diagram [squared] in the series is the probability of the particle undergoing said diagramatic evolution. The second equality groups up all diagrams into tree-level [no loops] and different loop level diagrams.

This encodes all possible ways the particle can interact with itself over time, thus all possible particle evolutions. We can also consider all possible ways two incoming particles interact in some way and outcome as two particles. This is captured by the 4-point function in quantum field theory [expectation value of four operators $\langle\varphi^4\rangle$ this time]:

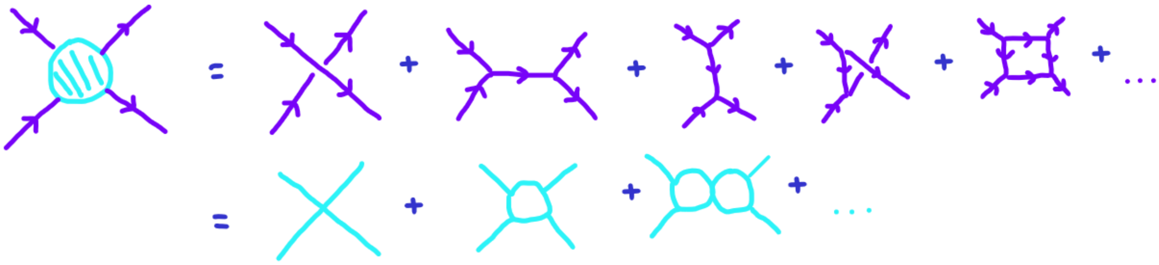

**Figure 8**. 4-point function for scalar particles. This represents all possible ways two particles can come in, interact in some way, and then outcome as two particles.

The different diagrams are given by permutations of combining different interaction vertices. Thus, an $n$-point function is a combinatoric expansion of $n/2$ particles interacting with each other as an addition of all possible diagrams. *Now what about the case of topological consensus networks?* We would like to encode all possible ways a network can evolve in time and interact with other networks given a fixed cobordism class $\Omega$ and boundary conditions $\mathcal{B}$. Analogously to quantum field theory, we would like an interaction vertex to prescribe how network histories may interact via permutations of gluing surgeries. We define such an interaction vertex for the topological consensus network as the 3-prong:

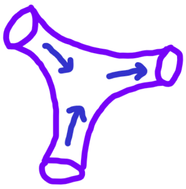

**Figure 9**. Topological interaction vertex of consensus networks, analogous to the vertex from $\varphi^3$ theory. From this we can combine it with other topological vertices to come up with all possible evolutions of a network, otherwise meaning all possible topological network histories in networktime.

With this we may describe *all* possible ways topological consensus networks can interact as a series of gluing surgeries between networks. Given a single network, how can it change in time given rounds of consensus which have the possibility of breaches in trust? We formulate this as the interaction of a single network history with itself as the series of cobordisms [of the same class]:

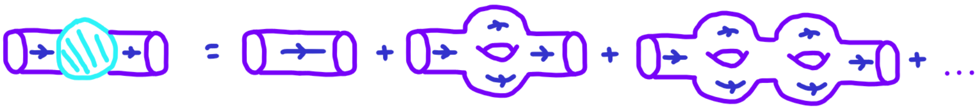

**Figure 10**. 2-point function for topological consensus networks. Given an initial and final state of a single consensus network, this combinatoric series represents all possible ways the network can split amongst itself into sub-networks, and then recombine into a single network. Furthermore, it demonstrates all possible trust breaching events following rounds of consensus.

More uncertainty in the trust of the network leads to increased splittings and, consequently, a higher genus. Accordingly we denote *branches* — independent networks evolutions from the same source — of interactions as more trustworthy given a minimal genus. Moreover, we can also consider how two independent networks [and hence their histories] can interact given consensus rounds. We characterize this by the diagrammatic series:

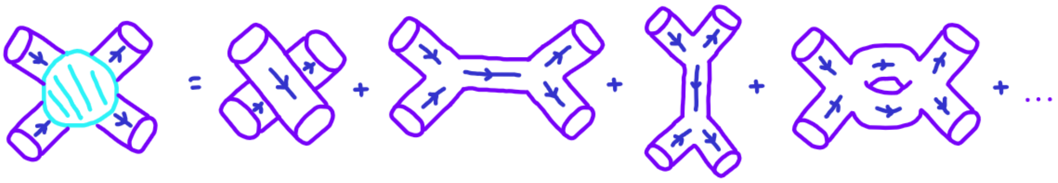

**Figure 11**. 4-point function for topological consensus networks. Given an initial and final state of a two consensus networks, this combinatoric series represents all possible ways the network can split amongst itself into sub-networks, and then recombine into two separate networks.

It is noted that the third term in the series represents part of networks *shedding* sizes. All diagrams are drawn with the same thickness as the diagram sizes of the initial and final networks are implied by the direction of flow. As another example, we can consider restricting our interactions to a cobordism class Ω that has three initial disconnected pieces, and one final. This would represent the way in which three separate networks interact to form a single network. Once again we represent it as the combinatoric series of surgeries:

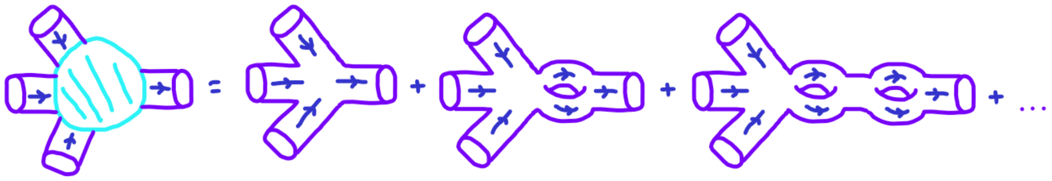

**Figure 12**. All possible evolutions of a system of three topological consensus networks ultimately combining into a single network after events of bifurcation for each consensus round.

*Thus the prescription for how networks interact and what information is required specifying unique network evolutions is given by the following.* Given an initial amount of independent topological consensus networks, one specifies a cobordism class Ω which has disconnected boundary pieces $\mathcal{B}$. For a class with $N$ initial networks [open boundary subsets] and $M$ final networks after interactions, we say we have an interaction of *type* $N \to M$ [the two and four point functions are denoted as $1 \to 1$, $2 \to 2$, respectively, while the interaction in Fig. 12 is written as $3 \to 1$]. After specifying the interaction type, we write all possible network evolutions of given boundary conditions of the disconnected pieces of $\mathcal{B}$ as a combinatoric series of cobordisms. We can compute the probabilities off all possible evolutions, and can select which to use to uniquely specify a network evolution. Now that we have such a prescription, we can look how it applies to **network autonomy**. For a given network $\mathcal{G}$ [and corresponding history $\mathcal{H}$], what possible histories does the network *want* to combine with? We would imagine one in a space of histories that is most trustworthy. We can characterize the *trust* of a network history by its *genus* $g$ — the maximum number of non-self-intersecting closed curves that one can draw on the surface without disconnecting it — given the topologies of its different branches. Thus a network searches for another network with minimal genus and checks if their type is compatible. For a network $\mathcal{G}$ of type $N \to M$, another network $\mathcal{G}'$ is *compatible* with it if the amount of incoming pieces of $\mathcal{G}'$ is the same amount of outgoing pieces of $\mathcal{G}$ [meaning the type for $\mathcal{G}'$ must be type of $M \to P$ for some arbitrary amount of outgoing pieces $P$]. This means that locally networks can specify a type and level of trust to autonomously interact amongst other networks without the need for external input. This interaction is captured by a diagramatic series of cobordisms in which interaction vertices are glued together. For a system of many independent networks, later we will see that the specification of a type will *additionally* require other information such as the topological invariants of the network histories. Next, we elaborate on the topological formulation of trust in terms of topological invariants in a continuous system.

### 2.3 Topological formulation of trust

In the first section we described trust as being characterized by the number of bifurcations formed after compliance checks at the end of consensus events. We attributed what is meant by trust to the genus of a network history. Although our system of nodes and transactions are inherently discrete, we opted for a *continuous* description such that we can define smooth network histories and make use of continuous topological invariants. Furthermore, we didn't explicitly discuss how one computes trust given arbitrary network history. We address these topics in this section.

#### 2.3.1 Continuous networks

First, we must justify our use of a continuum limit on a discrete system. Known as a *scaling limit* in mathematics, the continuum limit[†] of a lattice spacing [the distance between lattice sites] $\delta$ is the limit in which we take $\delta \to 0$. A popular application of this occurs when discussing discrete random processes such as Brownian motion which can be approximated as a continuous process for late times. For our case of a network history, then before the continuous limit we have a discrete set $\mathcal{Y}$ combined with a continuous set $\mathbb{R}$ as $\mathcal{M} = \mathbb{R} \times \mathcal{Y}$. If the spacing between transactions is given by $\delta_{\mathcal{T}}$ and the spacing between nodes is given by $\delta_{\mathcal{N}}$, then we say the continuum limit of this system is given by: $\delta_{\mathcal{T}}, \delta_{\mathcal{N}} \to 0$. Can we be more precise about this? Consider the *Whitney embedding theorem* [6]:

i) Any smooth real $m$-dimensional manifold can be smoothly embedded in $\mathbb{R}^{2m}$ [as the continuum limit of $\mathbb{Z}^{2m}$] for $m > 0$.

ii) Any continuous function from an $n$-dimensional manifold to an $m$-dimensional manifold may be approximated by a smooth embedding provided $m > 2n$.

[†] One could have for example a continuous quantum field theory as approximated by a lattice model in the limit where the lattice spacing vanishes. Such a process corresponds to finding a second order phase transition of the model.

For our purposes we will consider an embedding of our smooth topological consensus network in a higher dimensional discrete space for which we have taken the continuous limit. Now, what does it look like when we take such a limit? To answer this we will take motivation from *statistical mechanics.* Consider a discrete system of particles [an ensemble] of dimension $d$, linear size $L$ [the length of a side of the system], and correlation length $\eta$ [approximately the size of particles]. We say that the number of independent parts in this macroscopic system is:

$$N = \left(\frac{L}{\eta}\right)^{d}. \tag{2.10}$$

If we consider the system as having many possible states, then the total amount of possible states is a combinatoric result: $2^N$. The information of the dynamics of the system is succinctly captured by the *partition function* $Z$ which sums over all possible states of the system. If we denote the different states of the system as $\sigma$ [which can be interpreted for example as energy states $E_\sigma$] then we define the partition function as:

$$Z = \sum_{\sigma} e^{-E_\sigma/kT}, \tag{2.11}$$

where $E_\sigma$ is the energy of a given state, $k$ is the Boltzmann constant, and $T$ is the temperature of the system. From $Z$ we can compute many macroscopic quantities by differentiating it, and furthermore is used as a normalization for computing observables as expectation values. Now what if we wanted to take the continuum limit, how would this change? If we consider the volume of the phase space per particle as $V$ [hence the total volume of $N$ particles scales as $V^N$], we must take into account overcounting identical particles which comes with a factor of $N!$. Thus we say for the large $N$ limit, the total volume is given by $V^N/N! \approx (V/N)^N$. The volume of the phase space correspond exactly to counting all states of the system: $V^N = \sum_\sigma$. If we want to compute this for all particles in the system, then we must sum over all degrees of freedom. Being that we are working in the continuum limit [$N \gg 1$], this corresponds to integrating over all positions and momenta of the system as:

$$\sum_{\sigma} = \frac{1}{N!}\prod_{a=1}^{N}\int \frac{d\vec{q}_a\, d\vec{p}_a}{(2\pi\hbar)^d}. \tag{2.12}$$

Here then $\vec{q}_a$ corresponds to the $d$-dimensional position vector for the $a$-th particle, $\vec{p}_a$ corresponds to the momentum for the $a$-th particle, and the denominator is a normalization that comes from the Heisenberg uncertainty principle[†]. The measure $d\vec{q}_a$ can be equivalently expressed as $d^d q_a$. Our partition thus becomes in the continuum limit:

[†] The product measure over the degrees of freedom of the particles are precisely path integral measures in quantum field theory [related when rotating to real time via a Wick rotation]:

$$\prod_{a=1}^{N}\frac{d\vec{q}_a}{(2\pi\hbar)^{d/2}}, \prod_{a=1}^{N}\frac{d\vec{p}_a}{(2\pi\hbar)^{d/2}} \equiv \mathcal{D}\vec{q}, \mathcal{D}\vec{p}.$$

$$Z = \frac{1}{N!}\prod_{a=1}^{N}\int \frac{d\vec{q}_a\, d\vec{p}_a}{(2\pi\hbar)^d}\exp\left(-\frac{1}{kT}\sum_{a=1}^{N}H[\vec{q}_a,\vec{p}_a]\right). \tag{2.13}$$

Here $H$ is the Hamiltonian [roughly speaking the energy functional] of the system which contains the information of the energy states of the ensemble and hence all of its dynamics [the Hamiltonian generates time translations as given by Noether's theorem [7]]. Thus we see in essence the *continuum limit* amounts to a different way of summing the information of the system; we sum over infinitesimally separated pieces of information instead of summing discretely separated points. For our purposes then integrating over the phase space of the topological consensus networks amounts to:

$$\frac{1}{|\mathcal{Y}|!}\prod_{a}^{|\mathcal{N}|}\prod_{b}^{|\mathcal{T}|}\int_{\mathcal{Y}} dn_a d\tau_b. \tag{2.14}$$

Here $n_a \in \mathcal{N}$ is a node, and $\tau_b \in \mathcal{T}$ is an associated transaction. In the spirit of path integral measures, we shall define them as such:

$$\prod_{a}^{|\mathcal{N}|} dn_a, \prod_{b}^{|\mathcal{T}|} d\tau_b \equiv \mathcal{D}n, \mathcal{D}\tau. \tag{2.15}$$

Furthermore, since we are only interested over the topological consensus network $\mathcal{G}$ embedded in $\mathcal{Y}$, we will instead integrate over $\mathcal{Y}$ restricted over $\mathcal{G}$ [implicitly we assume whatever function we integrate over has compact support over $\mathcal{G}$]. Thus the phase space of a topological consensus network is given by:

$$V_{\mathcal{G}} = \frac{1}{|\mathcal{G}|!}\int_{\mathcal{G}} \mathcal{D}n\mathcal{D}\tau \tag{2.16}$$

If we wanted to integrate over the complete information of a network history, we need only include a temporal measure of the form $dt$ and thus integrate over $\mathcal{M}$ instead of $\mathcal{Y}$ [and correspondingly restrict this integral over the domain of compact support which is the network history $\mathcal{H}$]. Now that we have a prescription for taking the continuum limit of our originally discrete system, we should now discuss what is meant by *trust* and how we can compute it with phase space integrals. To evaluate the trust of a network from the perspective of another we require a classification of histories up to diffeomorphisms [isomorphisms or deformations of smooth manifolds]. We saw that breaches in trust result in bifurcation and thus the creation of non-trivial genus. In this sense we say that the **trust** of a topological consensus network history is precisely given by its genus. How do we characterize a genus of a manifold other than naively counting its holes? Incomes the *Euler characteristic* $\chi$. For us to understand this we must brush up on a few more topological concepts: *homology and cohomology.*

### 2.3.2 Trust via topological invariants

We motivated the use of equivalence classes of compact manifolds [cobordism classes $\Omega$] to describe the set of all topological consensus networks which can be deformed [evolved] into one another. We can infer more topological information from the network histories by studying other equivalence classes such as that of *forms* and *cycles*. For this we must look at *cohomology* and *homology* groups [8], respectively, over some history $\mathcal{H}$. We begin by introducing *de Rham* cohomology, followed by *simplicial* homology.

First, we motivate cohomology groups by looking at *vector spaces*. To look at a vector space over a history $\mathcal{H}$ is to look at a *decomposition with some sets of rules*. A vector space $V$ over $\mathcal{H}$ is constructed such that it is a decomposition into subspaces $\{V^a\}$ via summation:

$$V(\mathcal{H}) = \bigoplus_a V^a(\mathcal{H}). \tag{2.17}$$

Here $\bigoplus$ refers to summing the over the subsets $V = \sum_a V^a$ under which its elements [vectors] adhere to a uniqueness condition $\vec{v}^b \cap \sum_{a\neq b} \vec{v}^a = \{0\}, \forall\ \vec{v}^a \in V^a$. The uniqueness condition makes the summation what is called a called a *direct sum*. This is related to constructing representations in quantum theory as the sum of irreducible representations[†]. Over this vector space one has an orthonormal basis for $V$ written as $\{\vec{e_a}\}$ from which can decompose a vector $\vec{v} \in V$ as:

$$\vec{v} = \sum_a (\vec{v} \cdot \vec{e_a})\vec{e}_a, \tag{2.18}$$

for some real coefficients $c^a$. Typically the convention is to write $(\vec{v} \cdot \vec{e}_a) \equiv v^a$, where $v^a$ are the *vector components* of $\vec{v}$, and so with some shorthand notation — and dropping the vector hats — we instead have: $v = v^a e_a$ [where the sum is implied over $a$]. Where exactly do these vectors live? Consider a point $p \in \mathcal{H}$ such that we consider the tangent space at that point, $T_p\mathcal{H}$. The tangent space corresponds to a vector space in which all vector tails terminate at $p$, and all vectors are tangent to $\mathcal{H}$ at $p$. The basis of such is given by partial derivatives $\{\partial_a\} = \{\partial/\partial y^a\}$ for coordinates $y^a = (t, n, \tau)$, which correspond to elements in the time, nodal, and transaction dimensions $(\mathbb{R}, \mathcal{N}, \mathcal{T})$, respectively. In this we represent a vector as $v = v^a\partial_a$. *The logic behind the derivative basis is that it is the same as taking directional derivatives of functions on curves which give the tangential rate of change.* Consider the derivative of a function $f \in C^\infty(\mathcal{H})$ at a point $p \in \mathcal{K}$ in some curve $\mathcal{K} \subset \mathcal{H}$. Being that $\mathcal{H}$ is higher dimensional, the derivative of a function takes into account all the directions in which the function changes [as it is acted on by the flow which the tangential vector fields induce]. To select a *unit* direction $v$, we act the vector on the function in the form of a scalar product between $v$ and the gradient of $f$:

$$v(f) = v \cdot \nabla f = v^a \partial_a f = -v^t \frac{\partial f}{\partial t} + v^n \frac{\partial f}{\partial n} + v^\tau \frac{\partial f}{\partial \tau}. \tag{2.19}$$

[†] Consider two irreducible matrix representations [such as Pauli matrices for $SU(2)$] $\mathbf{A}, \mathbf{B} \in \mathbb{R}^{n\times n}$. To come up with a matrix that acts on an $n^2$-dimensional vector representation, we consider the direct sum of the irreducible representations as:

$$\mathbf{A} \oplus \mathbf{B} = \begin{bmatrix} \mathbf{A} & 0 \\ 0 & \mathbf{B} \end{bmatrix}.$$

Notice the minus sign in front of the first term as we are using Lorentzian manifolds to describe network histories. Here $v$ is in fact an operator which acts on functions $f$ in the form $v : C^\infty(\mathcal{H}) \longrightarrow \mathbb{R}$. We can write the components $v$ as $v = v^a\partial_a$, which acts on functions $f$ as $v(f) = (v^a\partial_a)f$. Thus we see in this case then the basis of which $v$ is expressed in is the basis of partial derivatives. More generally, instead of vectors we can instead have *tensors* which can be interpreted as higher rank vectors [such as matrices] which transform under the Jacobian. In this case instead of vector coefficients $v^a$, we instead have tensor coefficients $v^{a\ldots b}$. If the coefficients are symmetric such that $v^{a\ldots b} = v^{b\ldots a}$, then we may represent the tensor in the tangent basis:

$$v = v^{a\ldots b}\,\partial_a \otimes \cdots \otimes \partial_b, \tag{2.20}$$

where $\otimes$ is known as the *tensor product* which roughly speaking is a generalization of the outer product of vectors which allows you to combine the information of an arbitrary amount of tensors. If the coefficients of the tensor are antisymmetric such that $v^{a\ldots b} = -v^{b\ldots a}$ then we are instead working with a basis of *forms*. Forms $\omega$ are linear functionals which intake vectors to produce scalars such as $\omega(v) \in \mathbb{R}$. While vector spaces at a point $p$ — denoted as $V_p$ — are defined over the tangent space $T_p\mathcal{H}$, the space of forms $\Omega_p$ at a point $p$ are defined over cotangent spaces $T_p^*\mathcal{H}$. We denote the components of an antisymmetric tensor [a form] with lowercase indices as $\omega_{a\ldots b}$. We say that the tangent and cotangent spaces are **dual** to each other being that there is a relation between antisymmetric and symmetric tensors through a bilinear symmetric tensor known as a *metric* $g : T_p\mathcal{H} \times T_p\mathcal{H} \longrightarrow \mathbb{R}$. The relation is given as:

$$(g \circ \cdots \circ g)(\omega) = v, \tag{2.21}$$

where the number of compositions of the metric $g$ is given by the amount of indices [the *rank*] of $\omega$. While the basis of the tangent space is given by partial derivatives, the basis of the cotangent space will comprise of measures $dy^a$. What do these mean exactly? Recall from vector calculus that a change in variable $z^a = \gamma y^a$ — for some $\gamma \in \mathbb{C}$ — results in measures for integrals as $dz^a = \gamma dy^a$. These are in fact *exterior derivatives* $d$ [generalizations to operations such as gradients, divergence, and curl, depending on the dimension of the space] which act on forms [in our case coordinates]. To put explicitly, 0-form is a function while a 1-form is a function multiplying a basis measure such as $\omega = \omega_a dy^a$. A two form is a contraction of indices with two basis forms $\omega = \omega_{ab}dy^a \wedge dy^b$, where the $\wedge$ operation is known as a *wedge* product and is the anti-symmetrization of the tensor product $\otimes$. More generally, an $n$-form $\omega$ lives in the space of $n$-forms, written as $\Omega^n(\mathcal{H})$. Much like the decomposition of a vector space, we decompose the space of all forms over $\mathcal{H}$ as $\Omega(\mathcal{H}) = \bigoplus_a \Omega^a(\mathcal{H})$. An element $\omega \in \Omega$ can be expressed in the wedge product basis of 1-forms [measures]:

$$\omega = \omega_{a\ldots b}\,dx^a \wedge \cdots \wedge dx^b. \tag{2.22}$$

The relationship between the basis of forms and vectors is given as: $dy^a(\partial_b) = \delta^a_b$.

While symmetric vectors give us information of flow, forms give us information flow through pieces of space such as flux. The dual spaces — in the form tangent and cotangent spaces — are related via a musical isomorphism and so we can analogously extract information from either representation. Finally to discuss cohomology groups, we review some distinct sets of forms. If a form $\omega$ vanishes under the action of an exterior derivative $d$, then we call it *closed* such that $d\omega = 0$. If a form $\omega$ can be written as an exterior derivative of a lower rank form $\beta$ [such as $\omega = d\beta$], then we say it is *exact.* Let $C^n(\mathcal{H}) = \{\omega_n : d\omega_n = 0\}$ and $E^n(\mathcal{H}) = \{\nu_n : \nu_n = d\alpha_{n-1}\}$ be the set of closed and exact $n$-forms over $\mathcal{H}$, respectively. We can construct the $n$-th de Rham cohomology group over $\mathcal{H}$ as the quotient set:

$$H^n(\mathcal{H}) = C^n(\mathcal{H})/E^n(\mathcal{H}). \tag{2.23}$$

Here the elements of $H^n$ are equivalence classes of closed $n$-forms on $\mathcal{H}$, where the forms of the partitions are considered equivalent if they differ by an exact form:

$$\omega_n \sim \omega_n + d\alpha_{n-1}. \tag{2.24}$$

The cohomology group actually tells us quite a bit about the topology of $\mathcal{H}$, but this might seem too intuitive to think about this in terms of forms. We thus turn our attention to *simplicial homology* groups. Consider $n$-dimensional submanifolds $\{\mathcal{H}_i\}$ of $\mathcal{H}$, each labelled by an index $i$. We can consider what is known as an *$n$-chain* $a_n$, which is the sum over the submanifolds of $\mathcal{H}$:

$$a_n = \sum_i c_i \mathcal{H}_i, \tag{2.25}$$

where $c_i \in \mathbb{C}$ are coefficients. An *$n$-cycle* is an $n$-chain that does not have a boundary such that $\partial a_n = 0$. From this we will classify again a particular set of distinct cycles. Let $C_p(\mathcal{H}) = \{a_p : \partial a_p = 0\}$, and $B_p(\mathcal{H}) = \{b_p : b_p = \partial b_{p+1}\}$ be the set of $n$-cycles and $n$-boundaries [$n$-chains which are boundaries to manifolds] of $\mathcal{H}$, respectively. The $n$-th simplicial homology group over $\mathcal{H}$ can thus be written as the quotient set:

$$H_n(\mathcal{H}) = C_n(\mathcal{H})/B_n(\mathcal{H}). \tag{2.26}$$

Here the elements of $H_n$ equivalence classes of $n$-cycles of $\mathcal{H}$, where two elements of a partition are equivalent if they differ by a boundary:

$$a_n \sim a_n + \partial c_{n+1}. \tag{2.27}$$

While the equivalence of forms has no immediate physical interpretation, we can have some sense of intuition for equivalences in homology groups. Consider the homology of a torus as [8]:

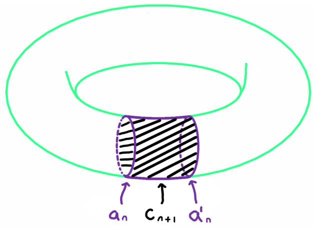

**Figure 13**. Visualization of the homology of a torus. Here $a_n$ and $a'_n$ are $n$-cycles of the torus [in our case $n = 2$], while $c_{n+1}$ is a submanifold of the torus. The cycles $a_n$ and $a'_n$ are equivalent up to the boundary of the submanifold which separates them, given by $\partial c_{n+1}$. Thus we say $a_n$ is equivalent to $a'_n \equiv a_n + \partial c_{n+1}$ as in E.q. (2.27).

*What does this have to do with topology?* Well first off we can construct the topological invariants based on these groups, which are quantities that are preserved under continuous deformations or diffeomorphisms of the space. For example, the dimension of the cohomology groups are the *Betti numbers* given by $b_n = \dim H^n$, which tell us the number of linearly independent harmonic[†] $n$-forms on $\mathcal{H}$. Additionally, this describes the amount of irreducible $n$-cycles of $\mathcal{H}$. The connection between the homology and cohomology groups of $\mathcal{H}$ is given by the *Poincaré duality*, which is an isomorphism between the groups:

$$H^n(\mathcal{H}) \cong H_{m-n}(\mathcal{H}), \tag{2.28}$$

which holds if $\mathcal{H}$ is a compact manifold for $m = \dim \mathcal{H}$, and $n \in \mathbb{Z}_+$. Although it might not seem too informative, the cohomology group tells us what forms[‡] can exist on $\mathcal{H}$, and the forms correspond to field operators in QFT. These field operators excite vacua to give rise to particles, and so we say the topology of the space $\mathcal{H}$ tells us exactly what kind of particles can exist on it. An example is the unit 2-sphere $S^2$ which has the Betti numbers $b_0 = 1, b_1 = 0, b_2 = 1$. Here $b_1 = 0$ tells us that $S^2$ does not admit a global 1-form or dual vector field, which is a manifestation of the *hairy ball theorem*. This is a direct result of the topology as if we punctured the unit sphere and deformed it to instead be a 2-torus $T^2$, $b_1$ would no longer vanish. In essence, the cohomology and homology groups tell us what forms and submanifolds of $\mathcal{H}$ are allowed to exist and in turn gives us information about it's topology.

Now, back to **trust**. Recall we defined the trust of a network history as given by its genus $g$ which is related to it's Euler characteristic $\chi$ via: $\chi = 2 - 2g$. Formally, we can write the Euler characteristic of a network history $\mathcal{H}$ via an alternating sum of its Betti numbers:

$$\chi(\mathcal{H}) = \sum_{a=0}^{\dim \mathcal{H}} (-1)^a b_a(\mathcal{H}) = \sum_{a=0}^{\dim \mathcal{H}} (-1)^a \dim H^a(\mathcal{H}). \tag{2.29}$$

Thus we say the *trust* of a consensus network history $\mathcal{H}$ is given by its genus:

[†] Harmonic forms vanish under the action of the Laplacian $\Delta$ as $\Delta\omega = 0$.

[‡] For each $n$-form we have a corresponding rank $n$ tensor field given by the *musical isomorphism* which maps between the cotangent and tangent spaces of $\mathcal{H}$.

$$r(\mathcal{H}) \equiv g(\mathcal{H}) = 1 - \frac{1}{2}\chi(\mathcal{H}). \tag{2.30}$$

A trusthworthy network is one which *minimizes* this quantity along the different *branches* [distinct network bifurcations of a given history]. What does trust look like for combined network histories which have interacted combinatorically? Consider indexing a set of network histories with indices $(i, j)$ and we select two such cobordisms $(\mathcal{H}_i, \mathcal{H}_j)$ which are compatible as they are of the same type. We glue them along open subsets $(\partial\mathcal{H}_i, \partial\mathcal{H}_j)$ with the use of diffeomorphisms $\phi = \{\phi_{ij} : \partial\mathcal{H}_i \to \partial\mathcal{H}_j\}$ mapping between them which we write as an identification $\partial\mathcal{H}_i \sim \partial\mathcal{H}_j$. Recall that their union — which we denote as $U$ — is defined in terms of a disjoint union modulo an equivalence relation on these open subsets:

$$U_{ij} = \mathcal{H}_i \cup_\phi \mathcal{H}_j = (\mathcal{H}_i \sqcup \mathcal{H}_j) / \sim . \tag{2.31}$$

How would one compute the Euler characteristic for such a space? Had we no identifications of boundary [i.e. the case of $U_{ij} = \mathcal{H}_i \sqcup \mathcal{H}_j$] then by the inclusion-exclusion principle of Euler characteristics, we would simply have $\chi(U_{ij}) = \chi(\mathcal{H}_i) + \chi(\mathcal{H}_j)$. However we have a slightly non-trivial case of identification which does not make us allowed to use that. For this we will make use of *Mayer-Vietoris sequences* [9] which provides a way to compute the cohomology of the union of two open sets [in our case is the disconnected boundaries of the network histories]. We can link $n$-th cohomology groups of histories using this as the exact sequence [a sequence of maps such that the image of one map equals the kernel of the next]:

$$\cdots \longrightarrow H^n(U_{ij}) \longrightarrow H^n(\mathcal{H}_i) \oplus H^n(\mathcal{H}_j) \longrightarrow H^n(\partial\mathcal{H}_i) \longrightarrow H^{n+1}(U_{ij}) \longrightarrow \dots . \tag{2.32}$$

From this sequence one can deduce based on arguments of dimensions of the cohomology groups that the Euler characteristics are related by:

$$\chi(U_{ij}) = \chi(\mathcal{H}_i) + \chi(\mathcal{H}_j) - \chi(\partial\mathcal{H}_i). \tag{2.33}$$

Note since we have the identification $\partial\mathcal{H}_i \sim \partial\mathcal{H}_j$, then equivalently the last term above can be instead written as $-\chi(\partial\mathcal{H}_j)$. Thus, the **trust of combined network histories** — for two network histories $(\mathcal{H}_i, \mathcal{H}_j)$ is given by:

$$r(U_{ij}) = 1 - \frac{1}{2}\Bigg(\chi(\mathcal{H}_i) + \chi(\mathcal{H}_j) - \chi(\partial\mathcal{H}_i)\Bigg). \tag{2.34}$$

It should be noted that the network history represents the understanding of trust for a given *perspective*, which can be the viewpoint of a single node, an entire network, or a client. For an $i$-th node of a topological network, we denote its trust in the $j$-th node as we $r_{ij}$. We say the total trust of node $i$ with all other $j$ is given by the trace $r_i = \mathrm{tr}_j(r_{ij})$, and [for the case of a non-topological network $\mathcal{N}$] with this we can compute the total amount of trust in a network:

$$r(\mathcal{N}) = \frac{1}{|\mathcal{N}|}\sum_{i=1}^{|\mathcal{N}|} r_i = \frac{1}{|\mathcal{N}|}\sum_{i=1}^{|\mathcal{N}|}\sum_{j=1}^{|\mathcal{N}|} r_{ij}. \tag{2.35}$$

In our case of a topological network $\mathcal{G}$, we must additionally include the information of the transactions to adhere to the 2D structure of the topological network, which we will label with indices $k$. We denote the trust node $i$ has in other nodes regarding transaction $k$ is given by: $r_{ik} = \mathrm{tr}_j(t_{ijk})$. Thus the total trust of a topological consensus network among its elements is:

$$r(\mathcal{G}) = \frac{1}{|\mathcal{G}|}\sum_{i=1}^{|\mathcal{N}|}\sum_{k=1}^{|\mathcal{T}|} r_{ik} = \frac{1}{|\mathcal{G}|}\sum_{i=1}^{|\mathcal{N}|}\sum_{j=1}^{|\mathcal{N}|}\sum_{k=1}^{|\mathcal{T}|} r_{ijk}. \tag{2.36}$$

One can consider trust that evolves in time which we represent via a discrete index $t$ and so our higher dimensional matrix of trust becomes $r^t_{ijk}$. The time index labels the different consensus [and so compliance check] events and so we say the trust in a network at a discrete time $t$ is:

$$r(\mathcal{G};t) = \sum_{t'=0}^{t} \frac{1}{|\mathcal{G}^{t'}|}\sum_{ijk} r^{t'}_{ijk} \tag{2.37}$$

Here $\mathcal{G}^t$ is the consensus network at discrete time $t$, and $t'$ is a temporary index to sum over all time until $t$. We convert the sums to continuous integrals over the phase space of the topological consensus network with the use of the continuum limit and instead recover:

$$r[\mathcal{G}](t) = \int_0^t dt' \, \frac{1}{|\mathcal{G}(t')|!}\int_{\mathcal{G}} \mathcal{D}n\mathcal{D}n'\mathcal{D}\tau \; r(t;n,n',\tau). \tag{2.38}$$

Here our discrete indices $(i,j,k,t)$ have been replaced with continuous variables $(n,n',\tau,t)$.

where $n'$ represents a node other than $n$. The equation for $r(\mathcal{G})$ gives us the trust in a topological consensus network at a given instance in time. As it evolves and bifurcates — forming a network history $\mathcal{H}$ — then the trust of its history is: $r(\mathcal{H}) = 1 - \frac{1}{2}\chi(\mathcal{H})$. One could imagine that the connection between the trust is that the information of its topology should agree with the individual trust of nodes in the network as it evolves in time. By this accord, we postulate for a time-dependent topological consensus network $\mathcal{G}(t)$ [which traces out $\mathcal{H}$], the total amount of trust in a history is given by the relation:

$$r(\mathcal{H}) = 1 - \frac{1}{2}\chi(\mathcal{H}) \overset{?}{=} \int dt \; r[\mathcal{G}](t). \tag{2.39}$$

## 2.4 Network-client product interface

What about an external system of clients? If we have some internal system of independent topological consensus networks [each evolving to trace out their respective histories], how can we utilize this to be used by some external client wanting to securely verify a given transaction? Well first me must consider that the notion of trust is **not** a local concept.

The network's local conception of trust given as a topological network history maybe not coincide with the client's external independent conception of trust among nodes in the network [much like how nodes have different levels of trust within one another]. Thus to make an autonomous system for clients to use, we must consider the intersection of trust among networks and clients. As an example, we can consider the scenario in which the network and client completely disagree on which subsets of networks are trustworthy:

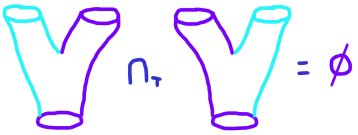

**Figure 14**. Null network history trust intersection. Sub-networks which are trusted are coloured magenta while un-trusted teal. The left prong represents trust based on the network's perspective while the right prong represents client's perspective of trust. The trust intersection [represented by the $\cap_T$ operator] is thus empty as the network and client completely disagree on which topological consensus sub-networks are trustworthy.

Alternatively, we can have a non-trivial intersection in which a subset of a trusted network is mutually selected from both perspectives:

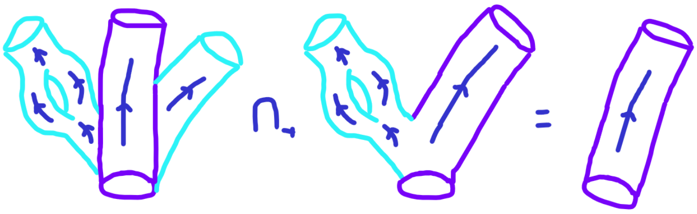

**Figure 15**. Real network history trust intersection. In this case on the left we have the network splitting into three sub-networks, two of which are un-trustworthy to different degrees. On the client's side, the rightmost [network] un-trusted network is in fact trusted. Thus the intersection is simply the trusted network as viewed by the nodes' perspective.

## 3 Trust dynamics of networks

To model the behaviours of networks bifurcating as cobordisms over time, we come up with algebraic expressions [with the use of algebraic topology] to describe the cobordism's geometric properties. With these equations we describe the dynamics of a topological consensus network to simulate breaches in trust and afford a more robust framework. We then fully classify an autonomous system of network histories and how they combine to demonstrate a proof-of-consensus service is possible in a scalable way with a quantum advantage.

### 3.1 Trust evolution of network interactions

### 3.2 Autonomous network classification

## A Topological quantum field theory

In this section we highlight how some of the topological framework used may be used to describe topological quantum field theory systems defined over knots in 2+1D. First we review some concepts in topology and then move onto the framework of topological quantum field theory and what we can learn from it.

## B Example Implementation

For a **regular** consensus network $\mathcal{N}$, we have a discrete set of nodes and so we take a consensus network to be a closed subset of the set of integers:

$$\mathcal{N} \subset \mathbb{Z}. \tag{B.1}$$

For a **topological** consensus network [in which we must work in at least two dimensions to have non-trivial topology], we combine the information of the nodes and transactions into a product space given by: $\mathcal{Y} = \mathcal{N} \times \mathcal{T}$, where $\mathcal{N}$ is the network and $\mathcal{T}$ is the space of values of trust. Each of these are given by $\mathcal{N} \subset \mathbb{Z}$ and $\mathcal{T} = [0, 1]$ [here $\mathcal{T}$ are continuous values between 0 and 1, also known as the closed unit interval]. Thus, a topological consensus network is thus a subset of the product space:

$$\mathcal{G} \subseteq \mathcal{Y} \subset \mathbb{Z} \times [0, 1]. \tag{B.2}$$

From this we can define a subjective interpretation of $\mathcal{Y}$ from node $i$ given as:

$$\mathcal{G}_i \subset \mathcal{Y}. \tag{B.3}$$

Within *either* type of consensus network, we can have some notion of subsets partially having trust in other subsets [this directly leads to bifurcations]. For now we look at the case consider the case of a network bifurcation from the subjective perspective of a **single node** $i \in \mathcal{N}$ [for a **regular** consensus network $\mathcal{N}$]. A node $i$ will have a subjective interpretation of trust in every other node $j$ in $\mathcal{N}$; we capture this information in a matrix $r_{ij} \in \mathcal{T}$. Consider this notion in some subset $S \subset \mathcal{N}$, then we say the total trust that node $i \in S$ has in the sub-network, $r_i(S)$, is given by the sum:

$$r_i(S) = \frac{1}{|S|} \sum_{j \in S} r_{ij}. \tag{B.4}$$

It is noted that $r_{ii} = 1$ is trivial as a node has full trust it itself. We can make *decisions* based on condition of this trust, such as deciding to cooperate with a sub-network given by the boolean function $f_i : S \longrightarrow \{0, 1\}$. We can represent this as a cutoff for acceptable trust as:

$$f_i(S) = \begin{cases} 1, \; r_i(S) \leq \delta_i \\ 0, \; r_i(S) > \delta_i, \end{cases} \tag{B.5}$$

where $\delta_i$ is some security parameter specified by the node $i$. The case $f_i = 1$ **implies** the existence of some subset $g \subseteq S$ that node $i$ wants to cooperate with. We can denote the subset as:

$$g_i(S) = \{j \mid r_{ij} \leq \delta_i\}_{j \in S}. \tag{B.6}$$

After a round of consensus occurs this gets updated and from the *perspective* of the $i$-th node, then ideally there would be a natural bifurcation into the subset they want to cooperate $[g_i]$ and its complement $\bar{g}_i = S \setminus g_i = \{i \in S | i \notin g_i\}$ [i.e. the rest of the network]. We present this updated network based on a bifurcation as:

$$S \xrightarrow{f_i} g_i \sqcup \bar{g}_i. \tag{B.7}$$

We may describe this bifurcation from a single network $S$ to a split disjoint union as a *cobordism* given by the following functional map:

$$\alpha : S \Rightarrow g_i \sqcup \bar{g}_i. \tag{B.8}$$

This traces out a network history given by $\mathcal{H}$ such that $\partial\mathcal{H} = S \sqcup g_i \sqcup \bar{g}_i$.

Now we move away from the subjective perspective of a single node to the subjective perspective of an **entire network** and their trust in another network.

Consider a node $i \in A$ [$A$ is some set of **clients**] and another $j \in S$. Trust of subset $A$ in subset $S$,

$$\begin{aligned} r_A(j) &= \frac{1}{|A|} \sum_{i \in A} r_{ij}, \\ r_A(S) &= \frac{1}{|S|} \sum_{j \in S} r_A(j), \end{aligned} \tag{B.9}$$

Define set-wise bifurcation with similar generalisation,

$$f_A(S) = \begin{cases} 1, \; r_A(S) \leq \delta_A \\ 0, \; r_A(S) > \delta_A \end{cases} \tag{B.10}$$

$$g_A(S) = \{j \mid r_A(j) \leq \delta_A\}_{j \in S}. \tag{B.11}$$

$$S \xrightarrow{f_A} g_A \sqcup \bar{g}_A. \tag{B.12}$$

We may describe this bifurcation from a single network $S$ to a split disjoint union as a *cobordism* given by the following functional map:

$$\beta : S \Rrightarrow g_A \sqcup \bar{g}_A. \tag{B.13}$$

This traces out a network history given by $\mathcal{H}$ such that $\partial\mathcal{H} = S \sqcup g_A \sqcup \bar{g}_A$.

Also, from this an *individual node $i$* decides whether they are willing to be a part of $A$ based on,

$$h_i(A) = \begin{cases} 1, \, \delta_A \leq \delta_i \\ 0, \text{ otherwise} \end{cases} \tag{B.14}$$

Now we can consider $r_{ij}$ as being a function of time such that $r_{ij} = r_{ij}(t)$ then we can have the information of a network splitting as some history $\mathcal{H} \subset \mathbb{R} \times \mathcal{Y}$. Before we had sets judging each other at an instant in time, now we have sets with their own history judging other histories. Consider two histories $\mathcal{H}$ and $\mathcal{K}$. What expression can we come up for the trust that $\mathcal{H}$ has in $\mathcal{K}$ which is written as $r_{\mathcal{H}}(\mathcal{K})$. Remember that $\mathcal{H} \subseteq \mathcal{M} \subset \mathbb{R} \times \mathbb{Z} \times [0, 1]$, where $\mathcal{T}$ is **trust**. Thus inherently then $r_{\mathcal{H}}$ is dependent on the value of the trust in individual nodes [in some explicit or implicit way].

## References

[1] D. Singh, G. Muraleedharan, B. Fu, C.-M. Cheng, N.R. Newton, P.P. Rohde et al., *Proof-of-work consensus by quantum sampling*, 2305.19865.

[2] J. Baez and J.P. Muniain, *Gauge Fields, Knots and Gravity*, World Scientific (Oct., 1994), 10.1142/2324.

[3] J.C. Baez and J. Vicary, *Wormholes and Entanglement*, *Classical and Quantum Gravity* **31** (2014) 214007.

[4] C.T.C. Wall, *Determination of the cobordism ring*, *The Annals of Mathematics* **72** (1960) 292.

[5] S. Smale, *On the structure of manifolds*, *American Journal of Mathematics* **84** (1962) 387.

[6] H. Whitney, *Differentiable manifolds*, *The Annals of Mathematics* **37** (1936) 645.

[7] E. Noether, *Invariante variations probleme*, *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* **1918** (1918) 235.

[8] P. Candelas, *Lectures on Complex Manifolds*, Springer-Verlag, 1st ed. (1987).

[9] A.I. Generalov, *Algebraic mayer–vietoris sequence*, *Journal of Mathematical Sciences* **264** (2022) 39–43.