Lakat

An open pluralistic base layer for academic publishing

Leonhard Horstmeyer
(Do not distribute)

June 10, 2023

Contents

Abstract

We propose a base-layer publication protocol for a permissionless, censorship-resistant, and decentralized network. The protocol is based on a directed acyclic graph (DAG) and is designed to be used as a base-layer for a decentralized social network. The protocol is designed to be used in a permissionless setting, where anyone can publish messages into the network. The protocol is designed to be resistant to censorship and denial of service attacks.

We propose a new consensus algorithm, called proof of review. In Lakat this algorithm is used to propose new states of a branch. It consists of review and a finality algorithm. We also propose a new finality algorithm, called lignification.

1 Introduction

With the vast amount of data structures, of query and storage systems, of versioning and networking tools and of large language models, one may engineer publishing systems by posing certain requirements that give rise to a different and arguably more collaborative, efficient and healthy academic culture. This approach can be contrasted with an incremental adjustment of the existing system, which in many quantitative sciences is called the greedy approach. We propose one such architecture around the available technology that we call *Lakat*. Lakat is a distributed database with a local peer-review concensus layer. The system serves as a permissionless continuous integration solution for collaborative research and one may conceptionally think of Lakat as a peer-to-peer version of wikipedia with a branch structure similar to git and a peer review system. Our starting point is a set of eight core requirements, that we posit for a publishing system:

1. **Open** – Content and code base[1] should be accessible freely[2].
2. **Permissionless** – No one should be barred from contributing.
3. **Pluralistic** – No monopoly on research opinion.[3]
4. **Process-oriented** – Emphasizing the process rather than an outcome.
5. **Conflict-oriented** – Making conflicts a feature rather than a bug.
6. **Curatable** – Making the organization of the content part of the output.
7. **Sustainable** – Data and compute resources should be low and reuse of fragments encouraged.
8. **AI friendly** – Allowing all kind of entities to contribute, indivduals, groups or AI agents.

The research paper as the gold standard of publisicing research output poses several threats to the overall scientific endeavour. It is a relict from the times where the printing press had been the latest innovation and where the channels for communicating had a large latency. We mention six issues associated with the paper-formatted research output that are addressed by Lakat:

- It incentivizes the creator(s) of scientific output to withhold preliminary results or results that are either not significant or at odds with a hypothesis. Even if there are significant results[4], they may not meet the eye or mind of other creators or consumers of scientific output until the entire paper has been published. It may then even take of the order of tens of months for the paper-formatted research output to be accessible, which is particularly problematic for impactful research. Thus the process of building on top of previous work and of critical engagement is hindered and in the best case deferred.

- It incentivize creator(s) to wrap minor changes into the costume of an entire research paper, reusing a possibly templated introduction over and over again.

- The output is but a polished snapshot of a process, an inorganic blob "data structure". The process of reaching a result or of not reaching it as well as the review process are generally not part of the output and not naturally representable in the rigid paper-format. The process often doesn't stop with the paper-publication, but continues thereafter and it requires awkward hacks in the form of addenda, corrections or new paper-formatted versions to account for changes.

- It creates rigid and isolated islands of content, disregarding potentially conflicting or agreeing intersections. Papers address these intersections with citations that are often placed in an unspecific context, and tend to reference an entire paper or body of work rather than a particular part. These intersections between different scientific outputs are not only constrained to citations, but entire paragraphs such as introduction or method sections are often simply replicated from previous papers. Thus, making conflicting or agreeing intersections a manifest part of the data structure can overcome the hacky fixes and shortcommings of the paper-format.

- The question of who contributed how much to a research output is often a source of conflict among researchers. A process-oriented publication system facilitates the tracking of contributions and may reduce the cases of unjust allocation of contributorship. In paper-formatted publications the contributorship is proxied by a negotiated ordered list of co-authors, which cannot capture contributions and inevitably leads to unjust allocations.

- The effective barring of potential contributors in paper-formatted research does not increase the level of scrutiny, creativity and quality of the output. On the contrary, maybe another set of eyes can add insights or expand on the results. Why should the self-declared co-authors be in the best position to conduct the

[1] Here we refer to the code base of any client implementation.
[2] Internet service providers are not free. So we refer here to additional charges.
[3] This is not not necessarily the same as "No single source of truth".
[4] These may be perceived as significant or later recognized as significant by the community

research? The fear for the theft of ideas is mostly inherent to bulk-publications and less to process-based research output.

Apart from the abovementioned problems with paper-formatted research, Lakat may also be instrumental for solving other problems with scientific publishing such as the exploitation of scientists regarding their review services and production of output. Even though Lakat does not address this directly, it does provide a base layer to build a system of incentives on top of it.

1.1 Related Work

There are various solutions that have been proposed to improve the process of science publishing with respect to transparency, review, ownership, decentralization, collaboration, openness or fairness. We exhibit proposed solutions and their benefits or shortcomings. Since Lakat sits at the intersection of branchable version control (c.f. git[](cite git)), large collaborative enyclopedias (c.f. wikipedia[](cite wiki)) and peer-to-peer (c.f. humans [](cite humans decentralization)) protocols (c.f. urbit [](cite urbit) or ipfs[](cite ipfs)), we will focus on solutions in that general triangle.

In 2006 the platform Scholarpedia [](find source) was launched. It is a wiki-based format with a peer review layer, where institutional affiliation is required for contributon. It is thus integrating a scholarly component into wikipedia. The required affiliation is also one of the drawbacks of this solution, since some potential contributors are barred. Furthermore, the authors of an article are either chosen or elected. This to our mind has two further problems. First, it raises the question who elects those that elect. Second, the collaborative dimension of wikipedia is lost. In contrast Lakat – like wikipedia – retains the permissionless so that no one is barred from editing or from proposing pull requests to change content (see Section **??** for details). In 2007 the Citizendium fork of the English wikipedia launched [] (find source) with the objective to add a quality assurance layer on top of wikipedia. The concept of approved aricles played an important role. However, who approves the articles. What happens to subsequent changes? Would they have to be approved again or does the approval yield a sort of finality for the manuscript? Another wiki-formatted solution is the Manubot platform [5], which allows for collaborative preparation of research articles that can then be sent to peer-reviewed journals. Manubot, however is not a publication platform itself but aids the collaborative process of reaching a classical publication.

There are also many attempts to put part of the existing publishing logic onto a cryptographically secured distributed ledger. Everipedia [] (find source) was a fork of wikipedia. They have also tried to build a quality assurance system on top of it using reputation tokens that can be staked and potentially lost in the process of edits, thus leveraging distributed ledger technology. So instead of tokenizing ownership of edits, they tokenized reputation. Those tokens were deployed on a blockchain (EOS and later Polygon). The project has been archived. Orvium [](find whitepaper link) on the other hand aims to put submission of manuscripts, revisions and publications onto a blockchain or at least have them stored using some decentralized storage provider. Unfortunately it is not evident who stores what, how and where. There is for instance not much information about whether they are creating a dedicated blockchain or use an existing one.(They also launched a designated token to further raise captial for their undertakings.) The Scienceroot project [](find source) was launched in 2018 with the intend to create an on-chain economy around the publishing system using a reward token called Science Token (ST) which is deployed on the Waves blockchain. They also created or attempted to create an academic journal that ties into their economy. Pluto [](find source) is a blockchain-based platform for academic publishing that supports peer review, open access and micropayments. ARTiFACTS [](find source) is a project that aims to create a blockchain-based platform for scholarly research that enables researchers to create a permanent, time-stamped record of their various items that support their research such as data sets, images, figures etc. PubChain [](find source) is a project that aims to create a decentralized open-access publication platform that combines a funding platform with decentralized publishing. Like Scienceroot, it has its own token coincidentally also called Science Token (ST), which is used to exchange funds, store articles on ipfs and store their content identifiers on the blockchain. They also plan to integrate crowdfunding through their marketplace. TimedChain [](find source) is a project that aims to create a blockchain-based editorial management system that organizes manuscripts by publishers, authors, readers and other third parties. EUREKA [6] is a project that aimed to create a blockchain-based peer-to-peer scientific data publishing platform with peer review, open access and micropayments. It was developed by the team behind ScienceMatters, an existing open access publisher that conducts triple-blind peer review. EUREKA also aimed to provide a blockchain-based rating and review system that allows readers to evaluate the impact of published articles. It is, however, not any more maintained. The Open Science company Desci Labs is developing a project called Desci Nodes [3]. Similar to Scienceroot, DeSci Nodes is a tool for creating research objects, which are a type of verifiable scientific publication that combines manuscripts, code, data, and more into a coherent unit of knowledge. The 2018 "nature index" article [1] entitled "Could Blockchain Unblock Science?" focusses on the question of how blockchain could be used to improve the process of current science publishing. Brock also mentions that data edits could be made permanently visible, which aludes to the idea of securing continuous editing in an immutable and consensual manner. He also developed and deployed the Frankl, which is an open

source blockchain-based publishing platform [2].

When developing solutions for academic publishing, blockchain technology seems appealing, because it yields effectively immutable globally agreed data in an open and transparent way without the need for a single source of trust. However, one must not fall into the falacy of searching nails for a hammer. At the heart of the blockchain paradigm lies the idea of a consensus about a global unique truth. This is a very useful technology for fiat (e.g. printed money or cryptocurrency), which exists through a global consensus. However, research output is not a fiat currency. It is subject to conflicting theories, opposing views and possibly irreconcilable results. All of those drive the continuous process that is science. One may build solutions on top of a blockchain to allow for potentially conflictual editing, but this is not what it was designed for. Instead we suggest to make Lakat a base layer that satisfies the requirements for a publication system by design.

There are also a range of solutions that attempt to decentralize version control systems or anchor them in a blockchain. One of the most prominent examples of a decentralized version of a version control system with branches is git-ssb [**?**]. It is based on the secure scuttlebutt protocol [**?**] and allows for distributed version control. The Radicle protocol [**?**] is a peer-to-peer network for code collaboration. It extends git with a networking protocol called Radicle Link. The project is governed through the RAD token, which is deployed on the ethereum blockchain. Both of the above are great tools for decentralized version control of code. However, they are not designed for the purpose of academic publishing. Another project that explores ways to decentralize the storage of versioned data is ceramic [**?**]. It is a decentralized network for managing mutable information. It is based on the idea of streams, which are append-only logs of JSON objects. The streams are anchored in a blockchain, which is used as a global ordering mechanism. The streams are stored in a decentralized storage network.

With the onset of large language models (LLMs) and AI agents that are capable of statistically extrapolating from a vast set of existing resources we are entering an era where some portions of the scientific research process can and should be outsourced to these models. Autonomous agents should be able to take part in the process of scientific discovery. The impact and power of AI-aided research can be seen in multiple forms and with the recent advances in the field of AI and the availability of large amounts of data its value for the scientific community only grows.

1.2 Imre Lakatos

The entire architecture of Lakat is heavily inspired by concepts developed by the Hungarian philosopher Imre Lakatos. In an attempt to contribute to the demarcation problem[] that was prominent in the field of philosophy of science during Lakatos' times, he developed the concept of a *research programme*[], which is also called *Lakatosian research programme* to avoid confusion with the colloquial use of the former term. The demarcation problem asks about the criteria which tell science apart from "pseudo-science". Lakatos develops his theory on the grounds of a process-oriented account of science. So rather than saying that this or that monolitic bulk of work or set of statements is or is not scientific, he posits that this distinction can only be made on the grounds of processes of theoretical amendments to an existing corpus of statements. He distinguishes progressive and degenerative amendments depending on whether they strengthen the programme's predictive power. For Lakatos a research programme consists of a *hard core*, which is a set of constituting assumptions, axioms as it were, that capture the essence of a research endeavour and a *protective belt* of auxiliary hypotheses. The key ideas that the Lakat-architecture takes from the concept of the Lakatosian research programmes are threefold: 1) The pluralism of various research undertakings. 2) The process-orientation 3) The distinction between a core and a protective belt. At the heart of these foundational concepts lies the idea that science lives through arguments, differences and discourse. The input of Lakatosian concepts into Lakat can then be described as follows: A research programme corresponds to a branch or a set of branches to which researchers contribute changes or ammendments. There is no single master branch, but rather every research programme has its own branch or set of branches. Conflicts with other branches or even within the same branch are an important aspect of Lakat and can be the source of progress (c.f. progressive ammendments in Lakatosian research programmes). A programme can maintain a set of feature branches that support the core branch. These side branches behave like a protective belt.

1.3 Overview

With Lakat we propose a manifestly pluralistic, process and conflict-oriented architecture for the continuous integration of publications with a primary use case of research publications. In this way Lakat becomes a living document. At its core the architecture consists of a linked data structure that resembles a DAG, where the key objects are branches. This data structure facilitates collaborative work in much the same way as git does. Branches may be thought of as the analogue of a journal in traditional publishing. The role of journal editors is covered largely by branch contributors. Branches are chains of blocks that contain submissions. Addition of another block happens via a proof of peer review, where the peers are the contributors to that branch. In that sense branches resemble blockchains with blocks consisting of submitted changes instead of transactions. As a consensus mechanism we discuss a solution that combines a proof-of-review at branch-level, a local (i.e. involving

just branch-contributors) consensus rather than a global one, with a new finality gadget called Lignification. The review process is open. In a first version of Lakat the identities of the reviewers and the creators of the reviewed content are disclosed, however we wish to migrate to a weak[5] form of a double-blind protocol leveraging zero-knowlege proofs, where each party may reveal their identity. Data is content-addressable and conforms to the ipld multihash format. Storage is handled by a networking component in Lakat which delegates the bulk of data storage to a selection of other storage providers, including decentralized storage networks such as ipfs, storj and others. This improves resiliance and longevity.

In the following we discuss the individual elements of the proposed system and highlight their interaction.

2 Data Structure

2.1 Bucket

The most elementary data object is the *bucket*. Each and every submitted item is submitted in a bucket: datasets, paragraphs, images and formulae are contained in buckets. These are examples of *atomic buckets*, expressing the fact that they are the building blocks of the system. Instead of a folder structure we solve the containment relation through designated buckets that we call *molecular buckets* (like *tree* nodes in git). The data part of those buckets contains merely an arrangement of atomic buckets. One may think of them as the analogue of an article, a book or some other curated content.

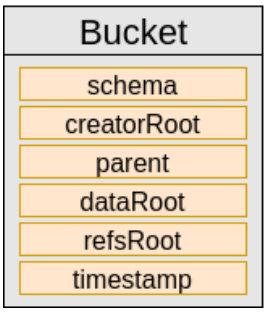

Figure 1: The most elementary type of data container is the bucket. It contains only immutable entries (orange), such as the *schema*, the *creatorRoot*, the *parent*, the *dataRoot*, the *refsRoot* and the *timestamp*.

Every bucket contains six entries: A *schema*, a *creatorRoot*, a *parent*, a *dataRoot*, a *refsRoot* and a *timestamp*. See Figure 1 for an illustration. Here and henceforth the word root refers to the root of a Merkle tree. We go through the entries in turn. The *schema* contains information about the format of the data. For instance we have already mentioned that the data in the molecular buckets is formatted as an arrangement[6]. The *creatorRoot* points to information about the creator of this bucket. Identity on *Lakat* is solved through proofs (see Section **??**). The *parent* is the *content identifier* of the parent bucket. For genesis buckets that would be 0. The *dataRoot* is a content identifier of the data contained in the bucket. In future versions the schema could be absorbed into the dataRoot using the ipld multihash format. This would require a Lakat-specific codec. The *refsRoot* points to all the references made to other buckets within the data. This is necessary, since references to other buckets might be obscured inside the data-encoding. This is an analogue of a list of citations. The *timestamp* records the time of inclusion of the bucket into the branch. It is important to note that we use ethereum block hashes as time stamps in our first version, since the local consensus is too weak to ensure that all participants are truthful to the time otherwise. Anticipating block hash is close to impossible. One cannot change the data inside the bucket. One would have to create a new bucket that points to the original bucket via its parent entry.

2.2 Branch

The central object type of Lakat is the *branch*. See Figure 2 for an illustration. Branches represent journals or research communities. They share some properties with *git*-branches and some with blockchains. Every branch contains an id, called *branchID*, that uniquely identifies it. The immutable entries of a branch and the initial head are hashed to produce the branch identifier. The branch also points to a parent branch from which it was branched off. This entry may however be empty for a certain type of branch, namely the sprout (see below). The corresponding entry is called *parentBranch*. This construction turns the set of branches into a linked data

[5]Weak is to be understood in the sense that both parties may choose to reveal their identity.

[6]The purposefully vague formulation of an 'arrangement' is due to the intention to keep that format flexible. One may think of this as an ordered list, but one might also consider further directives or clustering of content in a directed hypergraph.

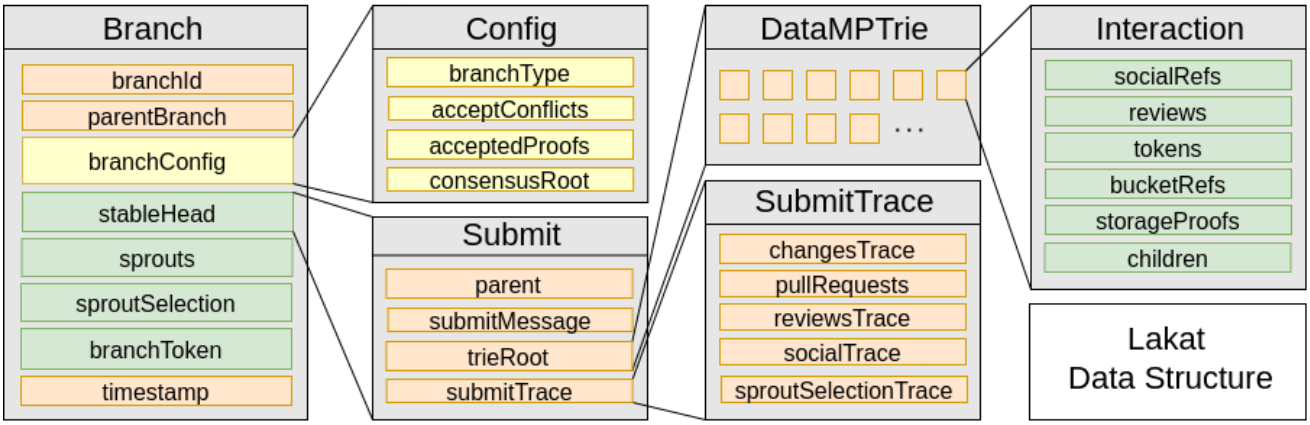

Figure 2: A schematic illustration of the branch object and its entries.

structure.[7] At creation time the branch receives a *timestamp*. The previous entries are all immutable. There are then four mutable entries, namely *stableHead*, then the two consensus entries *sprouts* and *sproutSelection* and finally *branchToken*. The stable head is a pointer to the latest stable submit. A *submit* is a set of changes (see Subsection 2.3 on submits). One may think of it as the Lakat version of an article submission. It has similiarities to a commit in git – not only phonetically – but also to a block in *ethereum*. The addition of new submits works through a consensus mechanism called *proof of review (PoR)* and *lignification* (see Subsection **??**). Also in this respect the branch behaves a lot like a blockchain. Every branch has it's own token, the *branchToken*. It allows funding bodies to fund a particular branch. Token logic is not handled by *Lakat*. Instead this entry essentially points to proofs of transactions on a blockchain where the respective token lives. The purpose of the integration of tokens is to create an incentive layer on top of Lakat, because (unfortunately) *humans* as well as *AI* do not work without incentives. The branch also carries configurational metadata, stored in *branchConfig*. It points to information about the branch type, whether merge conflicts are accepted (see Subsection 2.3), the consensus rules and the proofs that are accepted, such as proofs of token transfer or proofs of time. We use timestamps from latest blocks on various blockchains as proofs of time (see [4] and also opentimestamps.org). The branchConfig's mutability is more constrained than that of the stable head (See Subsection 4.6). Finally, we envision a way to extend the config schema. This would be done by an additional entry that points to a *schema bucket*, where the schema for the config is defined. An empty entry would signify the use of the default schema.

There are three types of branches: *proper branches*, *sprouts* and *twigs*. The branch type is stored in the branch config and can be changed under certain conditions. *Proper branches* can only be modified through the local consensus mechanism (see Subsection **??**). They point to a non-empty set of sprouts, which help with the process of producing stable heads in the proper branch. Proper branches cannot be changed to any other branch type. A *sprout* is a short-lived branch that is exclusively used to grow proper branches. Sprouts behave a bit like ommers in the ethereum protocol in the sense that they are contestors to produce the next stable head. They do not have an empty parent branch entry. Sprout branches point to an empty set of sprouts themselves. The sproutSelection contains all the sprouts that are rooted in it. The branchToken entries is empty. The stableHead is immutable. There is only one way to modify the sprout, namely indirectly when it turns into a proper branch during the lignification process (See Subsection 4.5). Once a sprout turns into a proper branch the parent branch entry is filled with the id of the branch that it is rooted in. Finally, a *twig* can be thought of a little feature branch. Twigs can be modified through submits by *contributors* of the twig (See Subsection 3.2 for more information on contributors) or through merges. However, the process of merging into a twig does not need to go through the consensus mechanism of proper branches (See Subsection **??**).

In this paragraph we merely introduce some nomenclature. We distinguish between *core* and *belt* branches, which correspond to *this* and *other* in git. These are not intrinsic properties of branches, but denote the role they play during a merge. Lakat only has one type of merge. The core branch will be updated and the belt branch not (see Susbsection **??** for information on merges). A branch may be a core with respect to one merge and a belt with respect to another merge. This terminology originates in the core-belt dichotomy of Lakatosian research programmes. There is a further distinction that is purely conceptual and is not manifested in the technical specification, but in the nomenclature. We distinguish a *derived branch* from a *seedling branch* in that the seedling branch has a *singularity submit* without a parent (See Subsection 2.3 for information on submits). A singularity submit corresponds to the genesis block in a blockchain. We invoke here a cosmological metaphore rather than a biblical one. The seedling branch has no parent branch and the corresponding entry points to zero.

[7] (Maybe check this) In *git* a branch is simply pointer to the head commit. In blockchains one often encounters ids attached to the chain (so-called *chainid*) to avoid issues when the consensus mechanism yields two differnt chains.

A derived branch on the other hand has a parent branch that it points to. We say that the derived branch is *rooted* in the parent branch. The *root* of a derived branch is the last submit in the submit history that is also in the history of the parent branch.

We also not that there are various levels at which Lakat can be viewed as a graph, going from high level to low level. At the level of the branches one can form a graph $\mathcal{B}$, where a branch is a node and a directed link from one branch A to another branch B means that B is the parent of A or that B is merged into A (See Subsection **??** regarding merging). This directed graph is not necessarily a-cyclic, because A can be rooted in B and merge back into B, however if one excludes merges it is. At the level of the submits, a graph $\mathcal{S}$ can be created with the submits being nodes and a link can be drawn from a submit q to p when p is the parent of q. This yields a directed acyclic graph (DAG). Finally at the level of the data buckets there exists a graph structure $\mathcal{D}$ induced by the parent reference inside the bucket. There is a graph homomorphism from $\mathcal{S}$ to $\mathcal{B}$, but not vice versa and there are no homomorphisms between $\mathcal{S}$ and $\mathcal{D}$ or $\mathcal{B}$ and $\mathcal{D}$. The lack of a homomorphism between the submit structure and the data structure indicates that these are two separate layers. The relation between the elementary bucket object and the higher level branch object is not simply a many-to-one relation. Different branches may share the some data buckets. In practice one would expect that most of the data inside a branch is shared with at least one other branch. See Figure 3 for an illustration of this relation.

2.3 Submit

Submits bundle up changes to the data with some additional metadata. Every submit points to a previous submit, the *parent* submit. There exist *singularity* submits that have no parent. The parent entry of those submits is zero. Like in git or ethereum, there is a field reserved for submit-specific data that we call *submitMessage*. The change of the data within the submit is subsumed in *trieRoot*, which is the root of the *DataMPTrie*, a Merkle-Patricia-Trie that references the data state of Lakat (see Section 2.4). The leafs of the trie are the data buckets. They have some resemblance with accounts in the ethereum state trie. Usually only a small part of the entire trie gets updated in a submit. Imagine the trie being all of wikipedia and a submit being just the creation of a new page or even just editing a page. Event though the bucket identifier is immutable it points to mutable entries. This is similar to ethereum, where the leave nodes are immutable account addresses that point to mutable entries like amount of ETH, the contract storage data or the account nonce. The mutable entries in the case of Lakat are made up of information that is attached by other users to the bucket. It is information that is not intrinsic to the bucket. This includes *socialRefs*, *reviews*, *tokens*, *bucketRefs* and *storageProofs*.

The socialRefs resolve to tokens of appreciation, such as thumbs up or down – the gold standard of social media user interaction. The reviews point to data buckets that contain a review or comments on the bucket in question. The tokens entry allow for the integration of tokens to data buckets. The bucketRefs are two collections of references to other buckets. The first collection is immutable and contains all those other buckets that are referenced inside the bucket data. This second collection is mutable and consists of all those molecular buckets that the atomic bucket is part of. This is a reverse registry that can be understood as how much a content has been reused. There is no analogue in classical publishing. StorageProofs are a ledger of timestamped proofs of storage for the bucket.

There are some submits with a specific structure. These are the *pull requests* (see Subsection 4.4) and the merge submits (see Subsection 4.7). The pull request contains at least one context bucket, called the *review container*, that references all the subsequent reviews. It also leaves a trace of the pull request in the submitTrace. The merge submit contains all the data buckets of the belt branch and it points to the merged branch id in the submitTrace.

In Lakat conflicts are at the heart of the protocol. They are cherished as the source of progress and sets Lakat apart from conventional publishing systems. We provide a clear definition of a conflict. A *submit conflict* with respect to a branch $\mathfrak{B}$ is a set of three submits π, s_1 and s_2 where π is the parent of both s_1 and s_2 and all three are included in $\mathfrak{B}$. We denote this 4-tupel by $(\mathfrak{B}, \pi, s_1, s_2)$. A submit that creates a submit conflict is called a *conflicted submit* and a submit that does not create a submit conflict is called *conflictless submit*. A *merge conflict* is a submit conflict that arises from a merge submit. Depending on the branch configuration (see Subsection 2.2) merge submits may or may not bring about merge conflicts.

2.4 Data–Trie

The data buckets as well as the mutable information attached to them can be looked up with the help of a Merkle-Patricia trie, called the *DataMPTrie*. This is cryptographically secure and very useful when resolving the information attached to buckets inside of an article. The keys that are stored in the trie are a truncated version of the content identifiers of the data buckets. And the values are the mutable entries attached to the buckets. To look up the bucket data itself one uses simply the content identifier of the bucket. Storage is handled separately (see Storage in Section 2.5). We propose to use a modified Merkle-Patricia trie – very similar to the one used in Ethereum – with four types of nodes: null nodes, leaf nodes, extension nodes and branch nodes []. The data

at each node is serialized and hashed. The specifics of this encoding are yet to be specified. One may use any of the existing ipld-formats. The encoding should have the property that data lists with a lot of empty entries are serialized in a very compact way to save space. Many data items in Lakat have a lot of empty fields. A bucket without any interaction information is mostly empty fields. A twig or a sprout have many empty fields as well. The leaf-nodes (in the trie) are special in this respect, because the hashing uses a salt that equals the content identifier of the bucket. Why do we need a salt at all? When a data bucket is published it doesn't have any information attached to it, so without the salt all new data buckets would have the same hash, which is not desirable.

2.5 Storage

The data is stored in key-value databases and is content addressed in the sense that the key equals the multihash of the data. We would like to use the ipld standard for linked data. Inside the multihash there is information about the storage protocols where the data is stored and can be retrieved. A piece of data can be stored with multiple protocols. A contributor may also choose to store the information on the own machine of course at the risk of having reduced uptime and not being discoverable. If one would use ipfs for storage then a certain flag in the multihash would be raised. If also another protocol or system would be used then this would again be seen through the flag in the multihash. The more branches point to a piece of data and the more subsequent submits rely on it the more important the persistence of that data becomes. The idea is that the availability, the longevity and the redundancy of data will scale with its importance in a self-organized fashion. A branch with many contributors will make sure to have the storage well secured and also well distributed. A newly created branch on the other hand needs to broadcast its creation (see Subsection 2.6 for branch creation broadcasting) to allow for distributed storage and attract contributors to ensure decentralized persistence of its data. This has two advantages. 1) Data that is pointed at by many branches is highly available and more redundant. 2) One cannot attack the system by creating lots and lots of branches. To proof that a certain data bucket has been stored, i.e. pinned, that proof is attached to the mutable information of the bucket in the *storageProofs* entry. There are a few more constraints about storage and pinning. It should be encouraged that every data bucket belongs to at least one molecular bucket so that there are no buckets without a context. Thus when a new data bucket is submitted the submission won't be accepted unless it is present in at least one context bucket.

When a new branch is created the data is initially just stored by the branch creator, but broadcasted through the network. Some nodes may pick up the data and store it as well. The branch creator may also choose to pin the data bucket in a certain storage system. Data that is close in the branch data structure is also close in the storage system. This is a very important feature of Lakat. It allows for a very efficient retrieval of data. The storage of data pertaining to a branch can be rewarded in branch tokens. This is not a feature of Lakat, but may be added on top of it to incentivize storage. There may also be a market for storage, where branch creators can

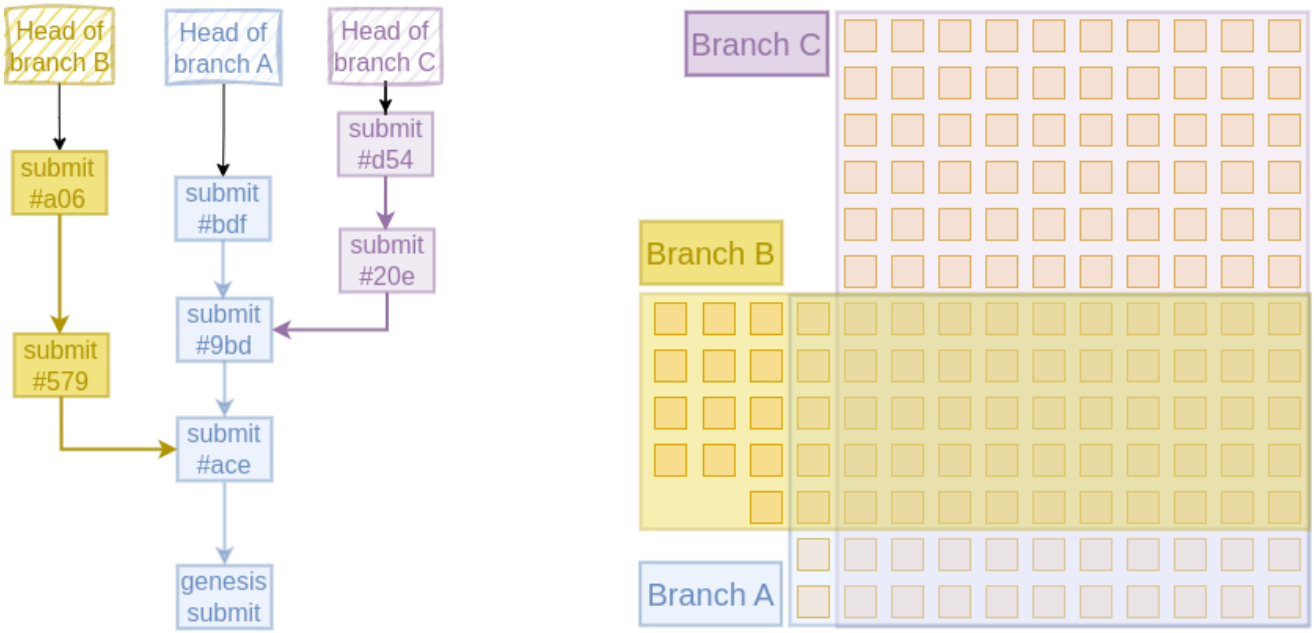

Figure 3:

buy storage space for their branch data. This is also not a feature of Lakat, but may be added on top of it.

2.6 Branch–Requests

Every branch has its own staging area, where any type of branch interactions are waiting to be included. This is called the *Branch–Requests* (or BR in short). It is similar to the mempool in ethereum. Everyone who is participating in the branch (See Protocol **??**) and who runs a light client may receive branch interactions from users and broadcast them to the network. Here we refer to a *client* as a piece of software that is yet to be written, which interacts with the network. A *light client* is a client that is not capable of doing branch operations, but is capable of receiving and broadcasting branch–requests. Inclusion of requests into the branch, however, requires more (see Protocol **??**). There are eight channels in the branch–requests (see Figure 4): *submit requests*, *pull requests*, *review commits*, *review submit requests*, *social transactions*, *token transactions*, *storage updates* and *branch creation broadcast*. The requests inside the BR are not permanently stored. Requests are kept for as long as any of the branch contributors keeps track of them. That is where the similarity to the mempool stems from.

Every channel in the Branch Requests has a certain capacity. In particular this aims to prevent that one channel clutters the entire pool of requests, which might happen if the capacity was channel-independent. All requests or broadcasts are serialized. Submit requests contain a serialization of the data buckets that are requested to be added to the branch. Pull requests are simply pings from other branches that seek reviewers. Only by means of a pull request are contributors from the target branch allowed to make modifications to the requesting branch (see Proof of Revie **??**).

(One can submit interaction data to any branch that holds it. Once a branch processes it,)

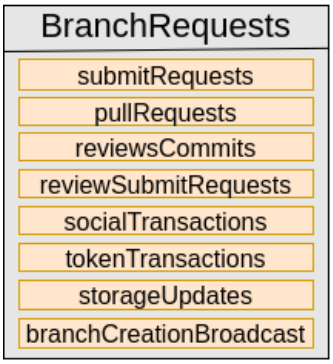

Figure 4:

3 Participants

3.1 User Identity

We propose to use an identity management system that ties in with some of the existing decentralized identity schemes and allows for the integration of multiple signing methods. For the first version of Lakat we propose to use 3id as the identity management system. 3id is a W3C compliant decentralized identity management system that allows for the integration of multiple signing keys. The identifier for 3id within the did system is did:3. It relies on a mutable document type in the ceramic network, called a stream. In the future we would also like to reduce identity to the ability to proof the submission of content without exposing further information about the identity using zero knowledge technology without a trusted setup. This would allow for a double blind review system. In order to publish content or send messages into the network a user needs to have an identity, which at this point is a did:3 identity registered in the ceramic network. The private keys in the did are used to sign messages and to proof authorship of content. The keys is also used to sign messages that are used to propose new states of a branch.

3.2 Contributor

Every branch has *contributors*, or rather contributors have branches. A contributor is an account that can prove to have contributed to a given branch. There are four types of contributors for any given branch: *content contributors*, *review contributors*, *token contributors* and *storage contributors*. A content contributor can prove to have submitted to the branch. A review contributor is someone who can prove to have pushed reviews to the

branch (see Subsection 4.4 for information on proof of review). A token contributor is someone who can prove to have deposited funds into the branch. A storage contributor is someone who can prove to store data of that branch. Being a contributor means that you have to prove your contribution for the submits from the root submit of the branch till the current stable head. How does the set of contributors change during a merge? What is the relation betwen the contributors of two branches before the marege and after? When the belt branch merged into the core following a pull request, then the new set of contributors is simply the union of the two branches (see Subsection 2.2 for the terms core and belt). That holds for all contributor types. When there is no pull request preceding the merge the contributors of this branch are unaltered. The main idea behind the concept of contributors is derived from the mutability, governance and autonomy of branches. Branches can only be modified by their contributors. This attempts to preempt attacks on branches.

3.3 Contribution

A contribution is any type of interaction with the branch. There are four types of contributions: *submit*, *review*, *token* and *storage*. A submit is a contribution that adds data to the branch. A review submit is a contribution that adds a review to a branch. A token submit is a contribution that adds a proof of a token creation, token mint or token transfer to the branch. A storage contribution is a proof about the storage of data pointed contained in the branch, i.e. pointed at by submits of the branch. A contribution is always associated with a branch and a contributor. In the first minimal viable version of Lakat, we are planning to use STARKs [] as proof system. This is due to the fact that STARKs do not require a trusted setup. We use Cairo programmes to generate proofs and point to their verification. The proof of contribution is a hash of the zero-knowledge proof of the contribution and its verification.

When a branch request is sent into the network it is being routed using the Kademlia protocol to the contributors of the corresponding branch. The backlog of requests is being shared and continuously broadcasted and updated by storage and content contributors using the libp2p library []. If the request has a payload that ought to modify the branch state, the receiving node checks the proof of contribution. If the proof is valid the node adds the contribution to the branch. If the proof is invalid the branch rejects the contribution. If the contribution is a submit and the submit is not valid it cannot be included in the branch.

4 Protocol

In this section we describe the Lakat protocol. We start with a high-level overview of the protocol and then go into the details of the individual components. Lakat is a shared key-value database of branches and data buckets together with a peer-to-peer protocol that governs the modification of this database. The modifications happen through submits to branches. The protocol needs to cover five functions: 1) Define a mechanism to construct new contributions [8]. 2) Broadcast information about requests and new branch modifications through the network. 3) Check the validity of the branch modification. 4) Define a strategy to finalize the state of a branch. 5) Incentivize contributors to propose modifications.

Lakat proposes a local consensus mechanism that relies on the notion of branch contributors. In principle Lakat could be used with various consensus mechanisms at branch level, such as proof-of-work or proof-of-stake. However, we propose a new one that we consider more suitable for academic publishing. This mechanism combines three concepts: 1) The distinction between *feature and production* branches 2) A *proof-of-review* mechanism that is used to propose new states of the production branch 3) A finality mechanism that is used to finalize the head of a branch, which we call *lignification*. The incentive mechanism is not built into Lakat, but may be added on top of it through the token handling at the level of the branch. Even in the current publishing business the incentives are outsourced to reputation, job promises and in some cases mere scientific curiousity. If anything, there is an anti-incentive to publish. In the following we describe the individual components of the protocol in detail.

4.1 Networking

On of Lakat's components is an asynchronous networking protocol, where peers can enter and leave at any time. The state of the individual processes of each peer is communicated and updated through a gossip protocol. The gossip protocol is used to broadcast requests and branch modifications to the network. We use the Kademlia DHT for this purpose. In Lakat the gossiping network is used to store the information state of the individual peers. This includes the branch requests (see Subsection 2.6) and the high level information the states of the branches that this peer keeps track of. This high level information consists of the branchId, the parentBranch, the branchConfig (branchType, acceptConflicts, acceptedProofs, consensusRoot), the stableHead (parent submit, submitMessage, trieRoot, submitTrace), the sprouts, sproutSelection, branchToken and timestamp (see Subsection 2.2). What about the bulk of the data, namely the data trie with all the data buckets and their respective interaction

[8] This is called block proposal for blockchains. Examples include proof-of-work or proof-of-stake

information, and the trace of the stableHead? That is optionally outsourced to other protocols. The protocols are then part of the multihash. They could include e.g. ipfs, filecoin, urbit[9] or if that peer chooses to do so, it could also store the data locally in the hash table. In Kademlia proximity of data is measured in proximity of the content identifier of the data. In future releases of Lakat we propose to tweek the proximity such that data stored on the same branch is close to each other. We are planning to use the libp2p library as a basis of the networking protocol. It is a modular networking stack that uses Kademlia.

4.2 Local Consensus

Who decides which content will be added to a branch? In lakat there is no global notion of what counts as science and what does not. There is only a local notion, the detailment of which is the subject of this section. A global consensus mechanism seems to be a good fit for a ledger that keeps track of values that are or ought to be globally agreed upon, i.e. for values that exist qua their global agreement. In contrast to money transactions, the global scope seems ill-fitted for the publication of research content. In our view this requires a local form of consensus. In the context of Lakat, the scope of the locality is at the branch-level.

What does a branch-level scope mean? This means that the scope is constrained to the *contributors* of a branch. Every branch has a history of submits and is *rooted* in some parent branch or is itself a *seedling* (See Subsection 2.2 regarding roots and seedlings). In either case there is a set of contributors to every branch between its root and the current head. Any actor, human or AI, who can prove to have contributed content in any of the branch's submits counts as a contributor (See Subsection **??**).

Branch contributors form the basis of the consensus mechanism. We entrench this deep into the protocol by allowing only branch contributors to make changes to the branch that they are contributing to. This design choice also keeps potential attackers from pushing unwanted content to a branch. Lakat does not make statements about what counts as science and what not. What counts as a legitimate scientific contribution purely emerges through the local consensus. One contribution that is viewed as being unfounded or unscientific for one branch might be viewed the opposite on another branch. In some sense this reflects a Feyerabendian approach []. It gives space for pluralism and allows for the organic selection of branches with possibly differing criteria on what counts as valid output. There is, however, a convergence in accepted method and output expected to emerge within a branch and also in branches that are close to each other. Branches that are close have branched off recently and possibly disagree more on technical grounds than on methodic grounds or they are simply feature branches that are to be merged back into the main branch soon. There is an overall incentive to merge branches, derived from the persistence of the data and the value of the token (see Subsection **??** for possible incentive structures).

The local consensus paradigm is governing amendments to branches, both to twigs and to proper branches. Sprouts on the other hand are just auxiliary objects that cannot be modified directly and are thus not amenable to a consensus mechanism. The consensus paradigm for twigs simply states that any branch contributor can push submits to the twig whereas merging into a twig requires a certain fraction of contributors to agree (See Subsection **??** for twigs and Subsection 4.3 for consensus on twigs). For proper branches the local consensus takes on a different form. It is divided into proof of review (See Subsection 4.4), broadcasting and lignification (See Subsection 4.5).

4.3 Feature Branches

Twigs are meant to be used for rather quick iteration. They behave like feature branches. Here is an example where twigs are expected to be used: If a contributor, human or AI, would like to add content to a target branch, say an article or some modifications or both, it creates a feature branch rooted in the target branch which subsequently goes through the proof-of-review consensus mechanism (see Subsection 4.4). Typically the number of content contributors on a twig will be low. Maybe a single author or a small group of authors, as it is the case for article publications. In order to not compromise the momentum and the quick iteration both content contributors and review contributors (if there are any) can push to the branch directly. Merges can also be pushed, but require a fraction of approvals of the content contributors. The fraction is determined in the config of the twig.

4.4 Proof of Review (PoR)

Before a branch can be merged into a proper branch it needs to undergo a review. Table 1 summarizes the steps. To start the review process an *issuing branch* creates a pull request from a *requesting branch* to a *target branch*. The pull request is a submit with two properties: First it contains a newly created context data bucket, called the *review container*, that will hold all the forthcoming information of the review. The submit may of course contain other buckets besides that. Second, it leaves a trace of the information about the pull request in the

[9] We also consider building on top of the Urbit OS using linedb[**?**] as a key-value storage and networking solution

#	Step	Description
1	Create pull request	The issuing branch creates a request for the requesting branch (in most cases identical) to be merged into the target branch. A review container is created.
2	Maturity of the pull request	The pull request is included in the requesting branch (in most cases immediate)
3	Commitment	A content contributor of the target branch publishes a review commitment to the requesting branch. That makes them review contributors of the requesting branch.
4	Review	The review contributors create review submits that are referenced in the review bucket.
5	Completion	The number of review cycles and the coverage of the review meets the criteria of the target's branchConfig. The branch may be merged into the target.

Table 1: Overview of the Proof–of–Review (PoR) process

pullRequests entry of the *submitTrace*, namely pointers to the review container, to the target branch and the requesting branch. In most cases the review happens on a twig, which acts as a feature branch. There the issuing branch and the requesting branch are identical, because the twig requests for itself to be pulled into the target branch. However, the requesting branch may also act as a proxy requester. This is the case when a proper branch rather than a twig seeks to be merged into a target branch. Since this intention itself must pass through the consensus rule of that proper branch, one would have to create a twig and include therein the proxy pull request. Once that twig is successfully merged into the actual requesting branch by passing the consensus, the review process can begin on that proper branch for it be mergeable into the target branch. We call a pull request *mature* once it is included in the requesting branch. In the most common scenario where the issuing and requesting branch coincide maturity is immediate. Once a pull request becomes mature a message will be send to the target branch where its contributors are invited to review the requesting branch. The message is simply a reference to the pull request sent to the pullRequests channel of the target's *branchRequests* (see Subsection **??** for branch requests). Any content contributor of the target branch who is not also contributing to the requesting branch can then become a *review contributor* of the requesting branch. They must first publish a review commitment on the requesting branch. This makes them official contributors to that branch. It also helps to gauge general reviewers engangement prior to the actual review. This is helpful both for those who seek to merge and those who seek to review. It also increases accountability of the committing reviewer. Failing to supply a review after a commitment could be penalized via the social engagement (see Subsection **??**). Committers publish their commitment in the reviewsTrace of the submitTrace. They cannot submit reviews without a prior commitment. Also, the identity of the reviewer is not public in the sense that the commitment solely contains a zero-knowledge proof that the reviewer is a contributer to the target branch (see Subsection 3.2). Of course the reviewer may decide to reveal their identity and this may or may not be in line with the configuration of the target branch.

Reviewers then push review submits to the requesting branch. The submits just contain a proof of contributorship in the target branch. A review submit consists of the following: A bucket with a review, called a *review item*. This bucket should reference all the data buckets that it has reviewed. In the respective interaction data (see Subsection 2.2) of all those reviewed buckets a reference to the review item is stored within the reviews entry. Finally the review item gets referenced in the review container of the pull request. Updating the review bucket, as with any bucket update, consists of creating a new review bucket that points to the old one through the parent entry[10]. The branchConfig of the target branch specifies the pre-requisites for a merge. This consists of the minimum number of reviewers, a rule for acceptance and a minimum number of review rounds, which could be one by default. The rule of acceptance could be preset aswell. For instance one could reject requests when a certain fraction of reviewers reject and accept when there are no rejections and specify some rule for the middle ground. Once all the requirements of the target branch are satisfied the branch is ready to be merged.

How about merging branches that do not seek to be merged? This can be the case when trying to merge the newest developments from a remote branch. This case is in fact already covered by the respective consensus mechanisms of twigs and proper branches. Merging into twigs requires a fraction of content contributors to agree (see Subsection 4.3). Merging into proper branches requires a pull request and subsequent reviews, so it is not possible to just merge other un-reviewed branches in the same way that one merges reviewed twigs or reviewed proper branches. Therefore, one would have to create a twig that merges the remote branch as a feature. It then requests to be merged und the merge undergoes a review. (clarify)

[10] In future versions of Lakat we wish to move to updates via deltas.

4.5 Broadcasting and Lignification

How are the reviewed pull requests bundled up and sequenced into a single proper branch? Why is the process important? How is the required attention bandwidth for this proess kept to a minimum? In order to explain the Lakat answer to this question we first contrast it to the case of blockchains: There transactions are bundled into blocks. They are then broadcasted across the network of nodes. When different blocks with the same parent are broadcasted, there will be conflicting versions of the blockchain state, which for a single source of truth is undesirable. In ethererum prior to the transition from the proof-of-work to the proof-of-stake these alternative versions were called ommers and were mostly the result of latency in the broadcasting, but of course also attacks or client-software issues. To make sure that a transaction has irrevocably been added into the blockchain one would have to wait for a few block confirmations.

In Lakat we solve the issue through a process that we call *lignification*. The idea is that amongst the potentially plentiful and conflicting versions of the new branch state eventually a new head will be chosen. This head is then called the stable head. The versions are stored as short-lived branches, called sprouts. The *sprouts* entry of the branch points to them. Why is the process of choosing a successor to the stable head important? Here is an explanation: The branch is an object that is kept alive by an ecosystem of contributors. It could get hijacked by a group of bad actors who became branch contributors through a mal-reviewed pull-request. In principle, if this happened, the contributors that disagreed with this malicious onboarding could bail out by creating a new branch. However, this new branch would have to grow the reputation of its contributors anew, seek new storage providers, have a new branch token and would generally have to start from scratch. It might not even be an attack, but a disagreement in the community that leads to a branching. Even though the process of finding a new stable head constitutes an important security measure for the branch, it should not create an overload of attention demanded from the target branch contributors. In most cases there will be no action required. But it is precisely those rare cases, where such a security measure becomes valuable. So one of the requirements for this process is that the branch production continues unambiguously when there is no interference from the community of contributors. In the following we introduce the process of broadcasting and lignification in more detail.

Broadcasting

Henceforth we refer to our proper branch as *core*. It functions as a production branch. Every proposed new merge submit could either become the stable head of core or become the first submit of a new (disagreeing) branch that is rooted in core. We refer to any of those new branches collectively as the *peri* branch. Not that the *core* branch may also become *peri* for another branch. Merge submits carry in themselves the possibility of becoming the head of a new branch. Therefore we decided to "wrap" them into short-lived proto-branches, namely sprouts, whose respective heads are the merge submits. The process of broadcasting is as follows. A content contributor of core, let's call her Alice, creates a merge submit, which is a special kind of submit (see Subsection 2.3 (ToDo)). This submit is then wrapped into a sprout, which means that the head of the sprout is set to be the merge submit and the content contributors are set to be the union of Alice and all the contributors of the pull-requesting branch. Let's call this sprout S. The branch information of the sprout becomes relevant if it eventually turns into a proper branch, a process which is discussed in the lignification part of this Subsection. The parent of the merge submit is the head of a branch B, that is either the core or any of the sprouts upstream of the core[11]. Alice chooses B, so she decides where to root the new sprout. If she decides to point to a branch that is already pointed at, there will be a conflict. The new sprout S – or rather its branchId – is then added to the sproutSelection entries of B and the sprouts entry of the core (which might coincide with B). The new state of core is then broadcasted to all contributors of core. Note that the new state of core might have received more updates than just the modification of the sprouts or sproutsSelection entries. There can also be further modifications resulting from the lignification process (see next part). The changes, i.e. creation, of the sprout branch S are also broadcasted to its contributors.

Lignification

Once a given submit is the new stable head of core or of peri, it cannot be revoked. We say it is *lignified*. The conversion of a previously flexible object into a rigid amendment of a branch has similarities to the process of lignification in botany. The decision about the stable head is not made immediately, but there is a period of time where it can still be revoked and deferred. This time is called *lignification time*. As mentioned above, the objects that we make decisions about are not the merge submits themselves, but the sprouts that contain them. If there is only one sprout available after the lignification time, then the decision is clear, namely that the submit contained in that sprout becomes the new stable head of core and no action is required. However, there may be multiple sprout options. In this case, we propose to have a deterministic rule that singles out one sprout and we suggest the possibility of vetoing the default deterministic choice. This minimizes the need to vote each time multiple

[11] The sprouts entry of a proper branch keeps track of all the upstream sprouts, but depending on the last branch update may also contain outdated sprouts. In order to retrieve all upstream sprouts one may "walk" upstream using the sproutSelection entry, which only contains the immediate offspring sprouts of a given branch.

options arise, but more importantly it reduces the attack vector for people to bring branch growth to a halt by proposing alternate – yet still reviewed – merge submits. Vetoing is possible throughout the lignification time. Any branch contributor may register a veto to any of the vying sprouts and therefore against the default sprout. In case that a veto is registered the sprout in question has a chance to provide the next stable head. (how does that work in practice and where is the veto registered and every proposal of new merge submits can also advance the state of the stable head ...) Once a veto is registered, the content contributors can bring in their votes on the rivaling sprouts. After a period of time, called the *engagement time*, the winning sprout will provide the new stable head and the other sprouts can turn into peripheral proper branches rooted in core. Like with blockchains, the state of Lakat does not change by itself, but only through transactions (See Subsection **??** for transactions). This means that only when a new submit is broadcasted can the state of a branch be updated. Furthermore, a branch may only be updated if it is the target of a transaction. If the transaction is targeting core, then peripheral branches cannot be updated and vice versa. As a consequence those ousted rivalling sprouts do not turn into their own branches immediately, but only once a transaction targets them. Some of them may never turn into proper branches at all. Apart from the lignification time and the optional engagement time there is a time allowing for latency issues in broadcasting, called the *broadcastingBuffer*. This ensures that the timestamped vetos or votes are broadcasted and thus recorded before the stable head is irrevocably fixed.

Due to the time between successive transactions it is quite possible that the state of the core, in particular its stable head, needs to be updated. Maybe the veto time or the voting time between rivalling sprouts has passed or maybe there are no rivalling sprouts and the stable head simply needs to be advanced. The speudo-code in the Lignification Algorithm 1 outlines the iterative procedure that advances the stable head on each new transaction. It is worth noting that also the sprouts entry and the sproutSelection entry of core get updated by pruning and replacement respectively. An illustration of the lignification process is also shown in Figure 5.

In practice the broadcasting and lignification can be automated by a script so that it requires less cognitive bandwidth. The script would choose a content contributor of core at random and broadcast collect all the pull requests that meet the merge-requirements from core, then create one or more merge submits from them, go through the lignification process and broadcast the result. Only in the case when there are disagreements would a manual interference be required.

4.6 Branch Config Changes

The branch config contains configurable metadata such as the branch type, a flag that can be set to allow only conflictless submits (see Subsection 2.3), then the accepted proofs (e.g. proofs of storage, proofs of contributorship, proofs of token transfer) and also the parameters that determine the consensus (e.g. the number of reviewers needed in the proof of review algorithm). These entries have constrained mutability. They require a merge rather than a plain commit to take effect. For a twig this means that the consensus mechanism for a twig needs to met, i.e. a config-specific fraction of contributors need to approve the merge. For a proper branch this means that the config change needs to go through the proof-of-review (PoR) consensus mechanism (see Subsection 4.4). We envision that in some future release there will be a default schema for the config, but that this schema may be altered through schema buckets to which the schema is pointing.

4.7 Branch Operations

Creation

The first branch operation is the creation. There are *genesis creations* and *rooted creations*. As the name suggest the genesis creation is a branch that does not have ancestorial submits. This is similar to blockchains or git, which have a block or submit without a parent. However unlike those Lakat allows for multiple genesis creations. Anyone can at any time create a new genesis branch, which is either a twig or a proper branch. A genesis creation requires the creator to set the branch config. Optionally the creator may also specify a branch token. On the other hand a rooted creation is a branch creation whose initial submit has a parent submit. There are two ways that rooted creations come about. One possibility is that a creator starts a new branch and chooses a parent submit as a root. Anyone may do that for any root branch at any time. The config can then either be chosen anew or inherited. Another possibility involves an ousted sprout, namely one that has been attempting to provide the next stable head in a lignification process. If that ousted sprout receives another submit, it turns into a proper branch. This branch is rooted in the branch for which it was a sprout. It inherits the branch config, but not the token and the branch contributors are the creator of the sprout and the content contributors of the branch that has been attempted to be merged. Any of those contributors can create submits to that ousted sprout and with that submit it turns into a proper branch where the parent entry is set during that conversion. Thus this mechanism for a rooted branch creation is indirect and can only be executed by the respective content contributors.

The creation of branches is permissionless. It is therefore a potential vector for a denial of service attack. The attacker can create a lot of branches and bombard other nodes with branch creation requests. One may leverage

Algorithm 1 Lignification – Advancing the stable head of the branch

```
Require: coreBranch, mergeSubmit, broadcastingBuffer, lignificationTime, engagementTime
  downstreamBranches ← branches downstream of coreBranch: [coreBranch, ..., sproutOf(mergeSubmit)]
  referenceBranch ← coreBranch /* referenceBranch may later be core or peri(pheral) branch */
  for i in 1 ... (downstreamBranches.length - 1) /* indexing starts at 1 */ do
    currentBranch ← downstreamBranches[i]
    childSprout ← downstreamBranches[i + 1] /* always exists */
    if all currentBranch.sprouts are within lignificationTime time (plus broadcastingBuffer) then
      return
    else
      if There is a veto against defaultSuccessor(currentBranch) and voting has finished then
        /* engagementTime is over (plus lignificationTime plus broadcastingBuffer) */
        if childSprout does not win the vote then
          /* doesn't participate (not defaultSuccessor or not part of a veto) or participates and doesn't win */
          childSprout becomes a peripheral branch rooted in referenceBranch.
          referenceBranch ← childSprout.
        else
          /* childSprout wins the vote */
          set the stableHead, sproutSelection and sprouts of referenceBranch to those of childSprout
        end if
        /* childSprout may or may not be defaultSuccessor. Both cases are covered. */
      else if There is a veto against defaultSuccessor(currentBranch), but voting has not finished then
        return
      else
        /* There is no veto against defaultSuccessor(currentBranch) */
        if childSprout is defaultSuccessor(currentBranch) then
          set the stableHead, sproutSelection and sprouts of referenceBranch to those of childSprout
        else
          childSprout becomes a peripheral branch rooted in referenceBranch.
          referenceBranch ← childSprout.
        end if
      end if
      /* Note that the referenceBranch may have changed. */
    end if
  end for
  return
```

the token entry in a newly created branch to mitigate this risk. The attachment of a proof of token transfer in the token entry of the branch can function as a filter for sincere branch creation broadcasts.

Merge

In Lakat a merge is the inclusion of changes from one branch into another. There is a strict directionality in a Lakat-merge. Git distinguishes between this and other and in Lakat this corresponds to core and peri, where core is the pulling branch. Merging into a proper branch can only occur after a pull-request (see Proof-of-Review in Subsection 4.4). Twigs on the other hand can pull other branches using an approval of a fraction of its content contributors. The fraction is specified in the branch config. After a merge the belt branch may become stale. A stale branch cannot receive submits. Whether a branch becomes stale after a merge depends on the branch config (see Subsection 4.6). A merge requires a merge submit (see Subsection 2.3) and a cryptographic validation of the branch that is merged. When the conditions for a merge are not met, the merge submit cannot pass the cryptographic validation. For instance if the config of the pulling branch only allows conflictless submits and the belt branch has conflicted submits, then the merge is invalid.

In order to discuss which data buckets are included in the merge submit we briefly introduce the set theoretic slang of A *minus* B for the set of elements in A that are not in B. The set of elements that are in A and B is called *intersection* of A and B and the set of elements that are in A or B is called the *union* of A and B. The respective notations are $A - B$, $A \cap B$ and $A \cup B$. We denote the set of submits of a branch $\mathfrak{B}$ by $\mathcal{S}_{\mathfrak{B}}$. We denote the set of data buckets in the data root of a submit s by $\mathcal{B}_s$. Thus the set of data buckets in a branch $\mathfrak{B}$ with stable head $head(\mathfrak{B})$ is $\mathcal{B}_{head(\mathfrak{B})}$.

We have already discussed that there is no many-to-one relation between buckets and branches (c.f. Figure 3). There may be data buckets in core $\mathfrak{C}$ that are not in belt $\mathfrak{P}$ and there sure are data buckets in belt that are not in

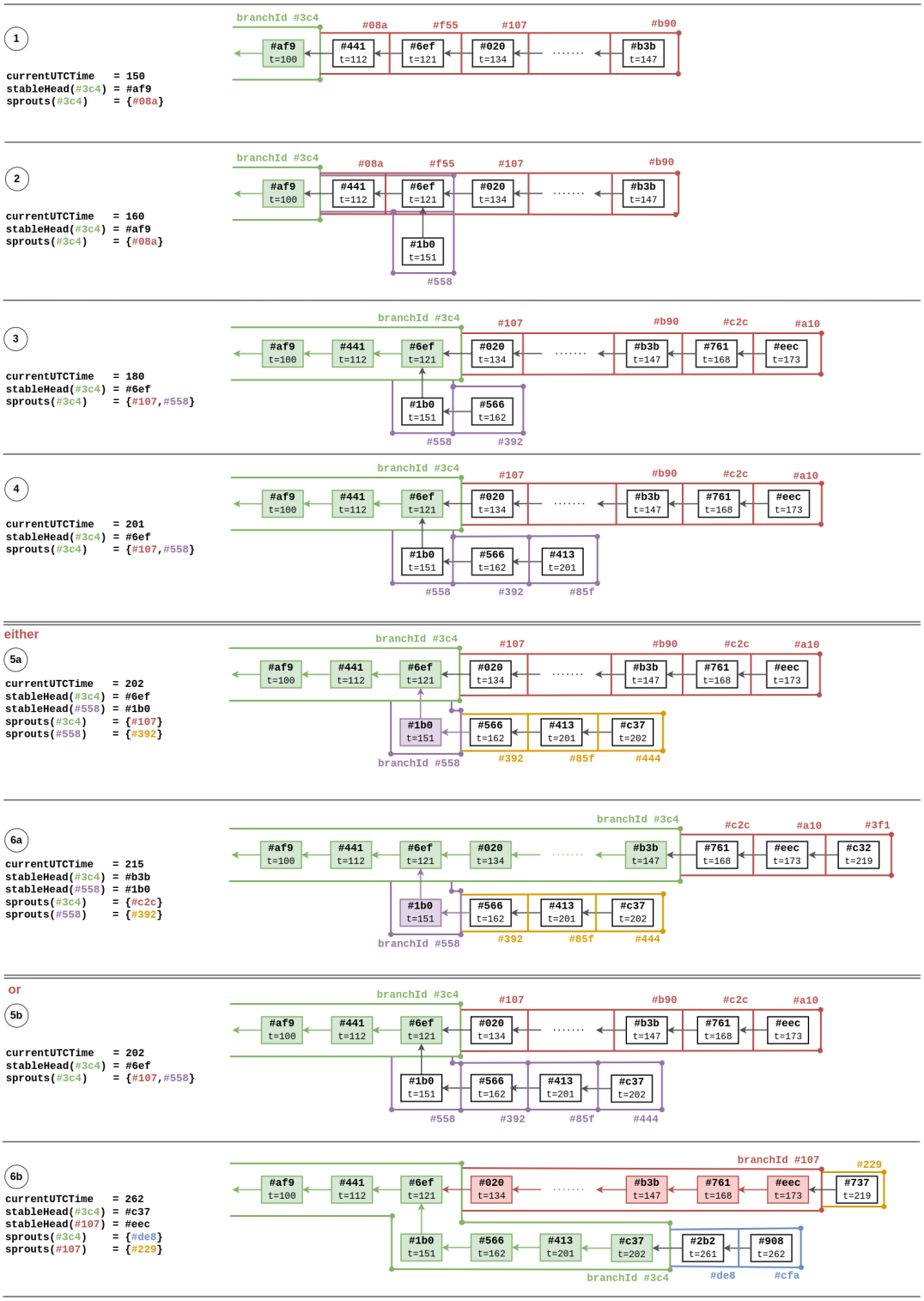

Figure 5: Example of a branch lignification with *broadcastingBuffer* = 1, *lignificationTime* = 50 and *engagementTime* = 60. Whenever a new mergeSubmit is added the lignification algorithm 1 runs and updates the stable head. The updates 1 to 4 are unambiguous. But then the target branch has two competing sprouts. The default sprout is *#107* and the other one is *#558*. Without any veto *#107* will deliver the next stable head of branch *#3c4*. This is the scenario 5a. The veto time plus *broadcastingBuffer* have passed and a new mergeSubmit *#c37* inside sprout *#444* triggers the lignification algorithm so that the loosing branch *#558* becomes lignified and rooted in *#3c4*. In 6a the mergeSubmit lignifies the target branch *#3c4*. Its head has advanced to *#b3b*. In scenario 5b a veto had been registered for *#558* in the sproutSelection entry of the target. If the voting turns out to be in favour of *#558*, the lignification process will grow the target branch in that direction (c.f. Step 6b).

core, i.e. $\mathcal{S}_{\mathfrak{P}} - \mathcal{S}_{\mathfrak{C}} \neq \emptyset$ is not empty. One question that arises in the context of merges is how to combine disparate bucket sets and how to handle that on the level of submits. There are two possible design choices. Either all the submits of belt become submits of core and consequentially also the buckets in $\mathcal{S}_{\mathfrak{P}} - \mathcal{S}_{\mathfrak{C}}$. Alternatively they stay submits of belt and the beforementioned buckets are included in the merge-submit's merkle hash of the data trie. In the first scenario one is faced with the problem, that the submits of belt all have immutable timestamps and parents. Rebasing those would require to loosen those immutability conditions. In the latter scenario one needs to point to the submits that whose data was included. It suffices to point to the peri's last submit before the merge. We opt for the second scenario. Unlike the first scenario, the second scenario has the peculiar situation that belt may have data buckets in common with core even though they do not share any submits, i.e. $\mathcal{S}_{\mathfrak{P}} \cap \mathcal{S}_{\mathfrak{C}} = \emptyset$ yet $\mathcal{B}_{\mathfrak{P}} \cap \mathcal{B}_{\mathfrak{C}} \neq \emptyset$. The only way this can happen in Lakat is if core and belt have pulled from the same branch or from branches that have a common submit in their histories [12].

5 Onramping

One of the objectives of Lakat is to transition academic publishing from a paper-formatted system to a cryptographically secure, collaborative and pluralistic system that allows for the continuous integration of research output. In order to achieve this objective, we believe that a transition should be as seemless as possible. The publishing system with isolated paper-formatted publications and intransparent review processes is an edge case of Lakat, an unsustainable and hacky one yet sufficient for onramping. We describe in which sense this is the case and how a transition could be achieved.

We can imagine a scenario for Lakat with a set of isolated branches. Each branch is controlled by a single legal entity, namely an academic journal. The academic journal is the content contributor, the storage contributor and the token contributor all in one. When a hypothetical researcher, say Alice (AI or human), wants to publish a paper, she has to send it to the journal. The branch that the journal controls is simply the indexed collection of articles that have been submitted, respectively chained together cryptographically. For a journal to transition its content to such a branch state is anywhere between immediate – by pointing the head of the branch to the storage locations of all content – or a matter of running a script that creates a submit for each accepted article retrospectively. Each paper is stored on a journal-controlled server, thus making the journal the sole storage provider. By adding the submissoin to the journal branch, the journal becomse the sole content contributor and retains all the rights of the contribution. The contribution is no longer owned by Alice at all. In this hypothetical oligarchic abberation of Lakat, a contribution is a submit with a single data bucket containing the paper. In summary, there is a way to map the classical publishing system into Lakat. Depending on the openness and licensing it might be difficult to either access or modify the content, but at least there is an entry point for the conversion. Why is this unsustainable? Given the design of Lakat, this branch would quite naturally undergo diversification through forking. At some point a researcher may create a branch routed in that journal branch, which is but a click. Maybe the incentive structure provided by the journal is soo strong that authors are willing to transfer all the rights to the journal voluntarily, but given Lakat's inherent ease of branching it will be a matter of time until there a diversification is to be expected.

6 Interfaces

We envision Lakat as a base layer for an open, pluralistic and collaborative publication system that progresses through continuous integration. As a base layer we strive to rely only on a bare minimum of other software and aim to have interface with for existing software or protocols. Here we provide an overview of the protocols and software that we plan to build upon or interface with.

We would like to interface with mediawiki. Mediawiki is an evolving database schema with a php frontend that allows for the creation of knowledge databases such as wikipedia. There are various ways how Lakat could interface with mediawiki. The weakest form requires the conversion of the data contributions in Lakat to database entries in mediawiki. A stronger form converts also contributions to mediawiki into Lakat contributions. Regarding storage we aim to stay agnostic and leave the storage protocol as a configurable option. As options we consider IPFS, Ceramic (which is built on top of IPFS and anchored in Ethereum) and Urbit (lineDB). Regarding the token layer we aim to be agnostic here as well. Since this is an optional feature it is left to the branch contributors to decide and merge updates on their token transactions into their branch. We do recomment to deploy tokens on Polygon though and plan to integrate this into the pipeline.

Regarding version control we would like to reduce the complexity of branch operations to a bare minimum in order to avoid security threats and reliance on other protocols. For the local consensus mechanism we believe that a heavily reduced set of operations is favourable. Nevertheless we would like to interface with existing version

[12] Here we make the distinction between the history of a branch and the set of submits of a branch. A branch may be rooted in another branch, but its history can go beyond the root.

control systems such as git or radicle. We would like to interface with them in order to allow for the conversion of git or radicle branches into Lakat branches.

We would also like to allow for new branches to be turned into parathreads in Polkadot. This would allow for the integration of Lakat into the Polkadot ecosystem. To this end one would need to create a pipeline to spin up a new parathread using Substrate together with a custom consensus protocol, namely the Lakat protocol. One would have to set the *BlockImport* to a custom way of importing new submits into the key-value database. *SelectChain* handles the finalization mechanism and would need to be set to the Lignification mechanism (See Subsection 4.5). One would also need to set the proof-of-review mechanism (See Subsection 4.4) in the *Environment* option of the Substrate runtime.

7 Conclusion

References

[1] Jon Brock. Could blockchain unblock science? *nature index https://www.nature.com/nature-index/news/could-blockchain-unblock-science*, 2018.

[2] Jon Brock. An open science platform. *whitepaper https://docsend.com/view/gn8t7k9*, 2018.

[3] DeSci Foundation. Desci nodes. *https://github.com/desci-labs/nodes*, 2022.

[4] Bela Gipp, Norman Meuschke, and André Gernandt. Decentralized trusted timestamping using the crypto currency bitcoin. *arXiv preprint arXiv:1502.04015*, 2015.

[5] Daniel S Himmelstein, Vincent Rubinetti, David R Slochower, Dongbo Hu, Venkat S Malladi, Casey S Greene, and Anthony Gitter. Open collaborative writing with manubot. *PLOS Computational Biology*, 15(6):e1007128, 2019.

[6] Andreas Schaufelbühl, Sina Rafati Niya, Lucas Pelloni, Severin Wullschleger, Thomas Bocek, Lawrence Rajendran, and Burkhard Stiller. Eureka–a minimal operational prototype of a blockchain-based rating and publishing system. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 13–14. IEEE, 2019.