Libertaria

Creating The P2P Economy For The Decentralized Society

HYDRA

Author:
Markus Maiwald
Contributors:
Dániel Róka, Attila Vágvölgyi

Abstract

As distributed ledger technologies such as blockchain move out of the proof-of-concept phase, they have run into a number of issues, such as scaling, many of which seem to have no clear solution. As teams rush to develop ever more complex technical workarounds to these problems, they appear to have missed the simple truth: not only do most of these problems arise from trying to do everything on a single chain, having everything on a single chain is a poor model for everyday human transaction and interaction.

While there is certainly a limited need for occasional global transactions, most people and communities make the same few types of transactions with the same few types of actors. By acknowledging that most transactions are local and within distinct communities, many of the problems of scaling and utility disappear naturally, without the need for advanced technical solutions.

By providing a set of simple protocols, Hydra will create a federated network of distributed ledgers known as journals, designed with the practicalities of human transaction in mind. The journals which form part of this ecosystem will all be able to interact with each other via the Hydra protocols, but most transactions will be limited to the individual journals themselves. This allows the network to scale without difficulty, and also provides trivial solutions to other problems which plague single-chain approaches, such as privacy, utility, and fairness.

As part of the wider Libertaria project, the whole network will be secured by a parent journal with its own token, Hydras (HYD). As well as providing security, the parent journal will provide a way for individual journals to interact, exchange value and access the wider Libertaria network.

Hydra is designed to be accessible to as many people as possible and address as wide a variety of needs as possible. To achieve this, Hydra provides ready-built components to build your own journal, whatever your requirements. Whether users need a permissioned company chain, local community currency or bitcoin-like open network, Hydra will provide pre-built templates for all the most common use cases.

Disclaimer

This vision paper describes a technology which is currently under development. While the philosophy and context underpinning the Hydra system is fixed, the precise implementation is certain to evolve as we continue to develop it. This paper should therefore be understood as broadly descriptive of our approach and ethos, and there is no guarantee that any specific feature or terminology listed below will persist to the final version of Hydra. As our approach solidifies, we will release updated documentation describing our progress.

Table of Contents

Introduction

What is Hydra?

Hydra is an economic protocol for transferring information and value. It is also a new approach to distributed ledger technology: a federated network of distinct blockchains, graphs and tangles all secured by a parent journal. Local communities can set up their own economies and tokens on their own journals, all in a few steps. The parent journal secures all the child journals, combining the power of all the nodes in the network. The parent journal can also be used to exchange value between different child journals in atomic swaps, but because these child journals represent local economies, most transactions stay on the individual journals. With Hydra, any community can run their own distributed ledger, getting all the efficiency benefits of keeping things local, while keeping the security and stability of a global system.

Key Features

Create your own blockchain: Use Hydra’s Genesis Templates to create your own blockchain or other ledger in just a few clicks.

Create your own token: Create any type of cryptotoken—whether it’s a utility, commodity, equity or something yet to be developed—and secure it with the consensus protocol of your choice.

Create your own community: Hydra protocols connect seamlessly with other Libertaria protocols, like governance, voting, law, smart contracts and more.

Fully scalable: Hydra scales globally while keeping most data and services local. Natural sharding without overcomplicating things.

Fully secure: Written in Rust to prevent memory and overflow issues. Journals are secured by the entire network while keeping all other features local.

A Note on Terminology:

While the majority of attention is currently focused on blockchain, a number of other distributed ledger technologies exist or are in development. While we expect blockchain to remain the most popular approach, at least in the short term, Hydra protocols are designed to be agnostic and to accommodate as wide a range of technologies and use cases as possible. Therefore, to avoid confusion, we use the term “journal” as a catch-all description of all current and future ledger technologies.

Current Challenges

Despite the rightful optimism surrounding blockchain and decentralized ledger technology in general, it is impossible to deny that current implementations are beset with problems.

Unfortunately, the hype which the industry has attracted in recent months has created a great deal of confusion and chaos. Not only is there little incentive to address these problems, very little work has been done to properly identify their true nature and scale. Instead, the discourse has descended into breathless and unhelpful polemic, with the majority of detractors dismissing blockchain and related technology outright and the majority of supporters mounting angry and righteous defenses based more on ideology than fact. As with all such debates, the truth lies somewhere in the middle.

Of course, these challenges are all interlinked, but they are divided below according to the categories most commonly ascribed to them.

Scaling

Hundreds of thousands of words have been written about the scaling issue, most commonly in relation to Ethereum or Bitcoin and its rivals. Yet the scaling problem is not monolithic: it is multifaceted and complex.

The most commonly cited scaling problem is transactional load, with many comparing the Visa network’s capacity (2,000 - 50,000 transactions per second) with Bitcoin’s (around 7 transactions per second). While this is important, there are many other issues which fall under the umbrella of “scaling”, including electricity use, full node storage requirements, governance and more.

A wide range of technical solutions to these various scaling problems have been suggested, including changes to chain parameters (block size, SegWit, etc.), off-chain solutions (lightning network, etc.), different consensus protocols (proof of stake, proof of tournament, etc.), different types of ledgers (tangles, DAGs, etc.) and different types of data partitioning (sharding, etc.). But few of these have been fully tested, and many introduce problems of their own.

Utility

Distributed ledgers are expensive and complicated compared to centralized systems. To justify this resource expenditure, the technology needs to provide sufficient benefits. But while there are many theoretical and ideological benefits to these technologies, current implementations are struggling to demonstrate this.

Accessibility

Distributed ledgers and their associated technologies are often claimed to provide significant societal benefits. But to truly provide these benefits, these technologies need to actually be usable by a wide range of people. There are two components to this issue: first, the technologies need to be accessible in the sense that they are simple enough for most people to understand and use. People don’t need to understand everything about how a technology works, but they need to be able to interact with them confidently, safely and easily. Some efforts have been made to smooth over the worst features here, and this will undoubtedly accelerate as these technologies become more mainstream, but the simple act of acquiring, transferring and using a cryptocurrency is still well beyond the expertise of most users.

But distributed ledger technologies also need to be accessible in an economic sense: the infrastructure and resources required to use them need to be within the means of most people, or they’re just another instrument for enriching the already powerful.

No current ledger technology meets both of these requirements, and most meet neither.

Fairness

Related but distinct from accessibility, a distributed ledger is only useful to most people if they can afford to actually use it once they have access. But huge global platforms which aim to process everyone’s transactions on a single chain or ledger via a system of transaction or gas fees will inevitably see the poorest users priced out.

Privacy

There is currently a great deal of confusion and misinformation around whether distributed ledgers are (or even should be) private. The transparent nature of distributed ledgers is one of their major features, but transparency and privacy are often directly at odds with each other. While auditability is important, people also have the right to privacy.

Governance, Disputes and Evolution

Decentralized systems are notoriously difficult to govern. Projects are hard to manage, easy to fork and incredibly hard to consolidate once forked, which is the worst of all worlds when it comes to stability and continuity. Many distributed ledger projects scale up quickly but then stall, because of a lack of long-term planning and few mechanisms for course correction.

Risk

In the rush to capitalize on the current cryptocurrency frenzy, very few projects are taking the time to consider their potential societal impacts. Decentralization is a powerful tool: once a system is decentralized it is difficult or impossible to stop. Blockchain and smart contracts are still in their infancy, and decentralized governance and reputation systems are barely embryonic. Yet already we're seeing ideas as reckless as trying to run countries' entire election system via the blockchain or putting millions of people's identities or medical records on chain. While these are certainly ideas worth considering and building up to, the risks of getting it wrong are considerable.

The Solution: Hydra

The Hydra protocols are designed to solve all the challenges listed above. Instead of focusing on a single issue and trying to cobble together a complex and untested technical solution, we take a pragmatic approach to the problem: What would useful journal technology look like? What features should it provide? What features are less useful or even unnecessary? While this may seem blindingly obvious, it actually stands in stark contrast to the common approach in the crypto space of building the technology first and only working out what it's actually useful for once things are too cumbersome to fix.

Hydra is designed to model and support standard human interaction and transactions. While this has certainly broadened with the development of technology, the fundamentals have remained unchanged for hundreds of years: the majority of transactions occur within distinct local communities and conform to a handful of types, with only a minority reaching outside these boundaries. While the rise of the Internet means that the definition of "local community" is now unconstrained by geography, online transaction and interaction is still mostly small-scale and tribal. The huge single-chain solutions offered by platforms such as Bitcoin and Ethereum simply aren't a good fit for how most people want to transact.

Hydra does not care:

- whether you have ten, ten thousand or ten million users,
- whether you want a blockchain or other type of distributed ledger,
- what you store on your ledger,

- whether you want a permissioned or trustless network,
- whether you want to develop your components from scratch, use the Hydra templates or mix and match the two.

The modularity and openness of the Hydra protocols provides the building blocks for all these use cases without locking users into a single globalized ledger that fails to fully meet anyone's needs. In doing so, it automatically and efficiently addresses all the problems outlined in the previous section.

Scaling

Hydra's approach to the scaling problem is fundamentally different from other distributed ledger technologies. Instead of asking "How do we scale?", the real question is "Do we need to scale at all?"

Having a global network of thousands of nodes certainly provides some advantages. Being geographically distributed makes the network secure against attack and censorship, and having a large number of nodes prevents against threats such as 51% attacks and other technical vulnerabilities. But beyond that, scale provides very little advantage. Why should records of local transactions be duplicated throughout the world, consuming precious bandwidth and storage, when the details of that transaction are of no interest outside the local community? Hydra is designed to scale only where there are tangible benefits, and keep everything else local.

Utility

Single-chain solutions try to cater to every possible user and end up satisfying none of them. By encouraging journals with a focus on local community, the Hydra protocols will create ledgers designed to solve specific issues faced by specific people.

Accessibility

By keeping individual ledgers small, resource requirements are reduced, allowing many more users to access the network. If communities have particularly low resource availability, they can create a journal to reflect that (e.g., by avoiding costly consensus protocols like proof of work).

Hydra's Genesis Templates (see below) make the network accessible even to non-technical users by providing standardized templates for common journal types.

Privacy

Focusing on smaller journals naturally resolves privacy issues. Journals which need to be fully private can be without accruing wider network costs, and the mere fact that transactional data is kept to within the relevant journals restricts the global flow of personal information.

Fairness

Because journals are distinct, users can no longer be priced out of using a journal by users from a completely unrelated marketplace. Local competition is rightly preserved, but communities which have particular fairness requirements can make journals to address these without affecting other users.

Governance, Disputes and Evolution

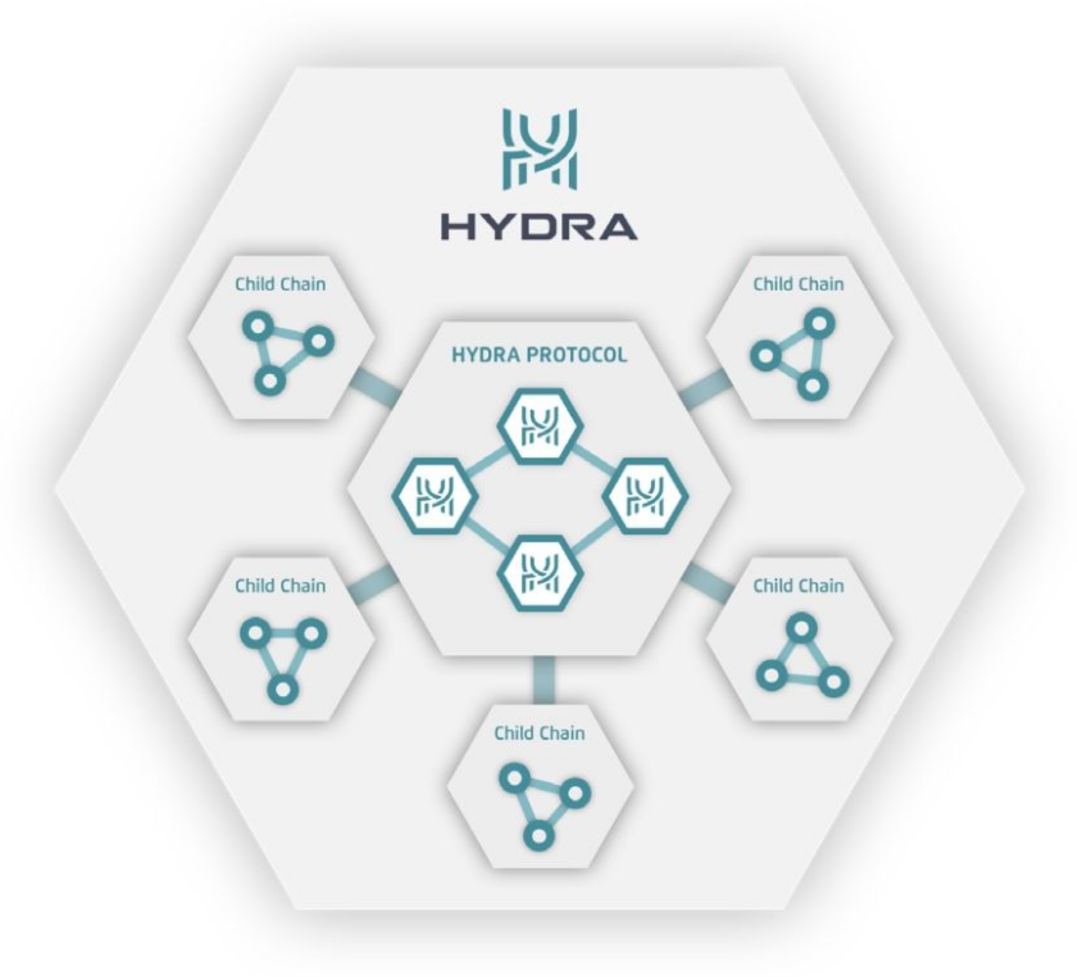
Hydra does not try to present a single journal as a solution to all problems in this space, but instead encourages diversity and natural evolution. New journals with new approaches can easily enter the space and experiment. Once they prove themselves useful, Hydra allows them to flourish in a diverse ecosystem of journals through cooperation, instead of forcing them all to run on the same platform (e.g., like Ethereum).

Hydra embraces diversity so much, that forking is a seamless and easy process. Forking is a sad event in the sense that a community is splitting, but differing views are very common, and providing an easy and convenient mechanism for splitting is better than having long disputes, fights and a cumbersome transition process.

In addition, because journals are smaller and more localized, forks will have fewer ramifications than they do on large single-chain platform.

Risk

Hydra provides the perfect environment as a testbed for new blockchain projects. Not every journal will succeed, and failure is a major part of innovation. By encouraging small-scale implementation, promising new uses of ledger technology can be trialed in small-scale environments, minimizing risk.



Hydra Features

Creating a Journal

Creating a new journal in the Hydra ecosystem simply involves creating a profile for this new journal inside the Mercury network (for more information on Mercury, see the Further Reading section, below).

This profile is similar to a genesis block, and will serve as a root for this journal. This root specifies all the characteristics of the journal that are required to come to consensus for the participants running this journal.

Journals can also be defined by forking off from other journals. In the case of a blockchain, the profile will refer to a certain block number of an existing blockchain as a starting point and define new consensus rules. Parties joining this new chain can clearly see the forking point, as this is part of the definition. This prevents replay attacks or duplicate copies of the block data on your hard drive.

Standardized Tools

Although they differ in their implementation, most journals will share common needs: storage, peer-to-peer protocols for synchronizing events, cryptography to authenticate participants, a consensus algorithm, ways to handle soft and hard forks, etc. They also require a vast ecosystem of standard tools to integrate them into applications, exchanges, wallets, voting tools, airdrops, etc.

Hydra will provide implementations for each of these needs along with ways for the open-source development community to audit, extend and reuse these implementations.

Genesis Templates

Hydra will also provide tools for non-developers to create their own journals. These are known as Genesis Templates. We will provide templates for a variety of use-cases that users can customize for the needs of their community, allowing them to create a custom journal in just a few clicks.

Inter-Journal Protocol

The Hydra inter-journal protocol allows a child journal to secure its historical data from long forks by registering checkpoints on a parent journal. This only makes sense if the nodes in the parent journal do not need to know the implementation details or the current state of the child journal. Thus, the inter-journal protocol provides a way for an individual, group or other entity to to secure the brand of a journal independently from the consensus algorithm which secures the journal itself.

This separation between the branding and consensus algorithm also encourages brand owners to listen to conflict within their community and resolve disputes peacefully, because making a new fork does not require any development effort.

The Hydra inter-journal protocol does not impose any requirements on the technology used by the child journals.

The Parent Journal

The parent journal secures all the child journals with its secure and reliable protocol.

Via the parent journal, the users of each child journal will have access to the complete Libertaria network and its large user base. Among other things, this will make it much easier to exchange value from one currency to another using Hydra (HYD), the token of the main parent journal.

Although the Hydra project will provide a journal designed to be used as a parent journal for most other journals, journals are not required to use it. Journals can decide to secure their journals by forming alliances and using their own parent-journal. A journal can even use multiple parent journals if they so desire.

Hydra Token

Overview

The Hydra project will provide a parent journal to support the various child journals. Other parent chains are permitted (and, indeed, encouraged), but the official Hydra parent journal is intended to be the primary backbone of the entire Hydra network. It will naturally have its own token, Hydra (HYD).

VERITAS ★ AEQUITAS ★ LIBERTAS
★ In Decentralisation We Trust ★

Token and Journal Philosophy

Hydra is being designed as a direct response to problems observed with first-generation distributed ledger technologies, such as Bitcoin, Ethereum, and others. While worthy attempts, these early blockchains have all suffered from either trying to do too much at once or being created with no clear use in mind and trying to arrive at a destination through trial and error. This ambiguity of purpose creates competing pressures which are destructive rather than constructive. And the results have been clear: wild volatility, dubious utility, creeping centralization, and crippling scaling issues.

Cryptotokens have many uses: they can be currencies, commodities, utility tokens, etc. There are countless use cases being worked on by projects across the cryptosphere and there will be countless more that have not yet been conceived of. But no single journal will be able to provide all of these use cases. In the fiat world, the financial system *as a whole* supports thousands of different types of value storage and exchange, but it does so with countless different types of financial instrument, each designed with a particular purpose in mind. In trying to improve upon this centralized old world, we should not abandon all the lessons it has taught us about how people transact.

Thus the Hydra network *as a whole* is designed to support broad experimentation in different types of token, but to achieve this the Hydra parent journal and Hydra token need to be designed with definitive purpose.

Crucially, the operation of the Hydra parent journal is designed to be automatic and apolitical. The Hydra network *as a whole* is designed to foster experimentation — even radical experimentation — across the whole political spectrum in all four pillars of a decentralized society (economics, production, communication, and law). To achieve this flexibility, the infrastructure which supports the network must be as robust as possible against political and economic influence from all sides. While the child journals should be able to fork easily, the parent journal should not. The following sections explain how we will achieve these aims.

Token Type

The Hydra token is definitively intended to be a commodity token, a stable store of value which will ensure the security of all the other tokens in the wider network. By deciding this from the start and designing accordingly, should avoid the problems which have plagued the more generalist approaches.

Supply

There is an initial coin supply of 33,550,336 HYD. This figure has been chosen for a variety of practical, mathematical, and economic reasons. These initial coins are intended to bootstrap and Hydra network, support the creation of the initial child journals, and fund development of the various technologies needed to create the whole Hydra network.

Cryptocurrency developers have quickly had to learn a great deal about the messy world of monetary policy. The arbitrary ability to print currency and flood financial systems with new money in the form of banking debts is certainly responsible for a great deal of the problems cryptocurrencies are hoping to fix, but an inflexible money supply is not much better. This is most clearly seen with bitcoin, where the function for how the token supply would change with time was fully laid out in advance by the creator, and users now have only the crudest tools available to combat runaway demand. A balance is needed.

Therefore, Hydra will adopt a dynamic approach to coin supply. As communities, companies, and hopefully even governments decide to create journals in the Hydra network, they will bring external value to the system and demand for Hydra tokens will increase. When this happens, the supply of Hydras will increase to offset any extreme demand pressures and associated unwanted price fluctuations. The amount of this supply increase will vary based on the external value being added to the network by the new child journal. Our developers and mathematicians are still working out the precise functions for determining these supply increases, but we are hopeful that this system will strike a much-needed balance between the arbitrary nature of the old financial system and the inflexible approach taken by first-generation blockchains.

Consensus Mechanism

To support the entire Hydra network, the Hydra parent journal needs to be secured by an extremely robust and efficient consensus mechanism. Proof of work is the approach which comes closest to our needs, but the resource consumption and mining centralization problems inherent to this technique are insurmountable. Therefore, we have developed a new approach based on the Algorand protocol described in Chen and Micali (2017). Algorand takes a randomised approach to verifying a ledger, dramatically reducing computation requirements, the probability of forking, and dispensing with the need for miners.

Hydra Details

Name	Hydra (HYD)
Currency Symbols	Ħ / ħ
Total Initial Supply	33,550,336 (increasing as child journals are formed)
Decimals	8

Integration with Libertaria

The federated Hydra network is part of the wider Libertaria project. As such, it is optimized for use with other Libertaria technologies such as the Mercury person-to-person communications protocol and the global network of nodes running TitaniaOS. However, journals are free to integrate with whichever technologies they desire. More information on the Libertaria project can be found in the Further Reading section, below.

Independent ledgers that protect each other are a vital part of the decentralized person-to-person economy, the second pillar of decentralization as defined by the Decentralized Society.

Further Reading

Official & Social Media

- Libertaria website
- Libertaria on Twitter
- Libertaria on Facebook

Papers

- Libertaria blue paper
- Project Mercury white paper
- Project Titania white paper

Libertaria on Medium

- Libertaria on Medium

General articles

- Libertaria technical overview
- Libertaria, the decentralized society

Decentralized Society

The Decentralized Society is a foundation dedicated to research and writing about decentralization.

- Decentralized Society on Twitter
- Decentralized Society on YouTube
- Decentralized Society Manifesto