THE BOOK OF HOPR

CHANGING DATA PRIVACY FOR GOOD

hopr

v1 January 2021

CONTENTS

HOPR – A SAFE AND SECURE INTERNET BY AND FOR US ALL

hopr

HOPR‘s Mainnet Launch was codenamed Jungfrau, after the famous Jungfraujoch mountain in Switzerland.

EXECUTIVE SUMMARY

let’s buidl the future together!

Imagine a world in which everything you did, from the time you wake up in the morning through when you go to bed at night, left a permanent record. Now imagine that almost anyone with the right technical skills could read this record and build a dossier on your daily life. This is the reality of the Internet today.

While people are aware of the need to protect their personal data online, few realise that there is a huge privacy hole baked into the fabric of cyberspace. We are talking about the ability of observers on the Internet to freely track the metadata associated with online activity and use it to deduce a great deal of information about who we are, what we are doing, even what we are thinking. While rarely talked about, “metadata surveillance” is one of the greatest threats to public and commercial privacy today, allowing savvy observers to spy on all Internet traffic regardless of the security precautions users might take.

The HOPR project aims to give people an alternative by providing an easy and cost-effective way to protect their metadata. Such network-level privacy will allow everyone - whether individuals, companies or organisations - to use the Internet safely and securely, as is their right.

HOPR achieves this in different ways. The **HOPR protocol** provides an alternative infrastructure on top of the Internet that makes metadata surveillance impossible. The **HOPR network**, a decentralised, peer-to-peer network that is managed by its users, keeps HOPR independent and free from the influence of a central entity. The **HOPR token** helps this network be financially self-sustaining by providing a means of payment for users and a revenue opportunity for anyone who wants to run a HOPR node. It also provides

the basis for participation in the **HOPR Association**, the independent DAO governing HOPR and run by its users.

In this paper we provide a high-level, non-technical and accessible overview of why HOPR is needed and how it works. We also explain how anyone who wants to can participate in the network, earning financial rewards while helping the cause of Internet privacy.

We start by examining the metadata problem. The information that accompanies every packet of data that is sent out on the Internet, metadata is used to route Internet data to its proper destination - a bit like an envelope does for the letter inside it. We show how metadata can reveal much more information about the sender, receiver and even contents of the data packet than most people are aware, and how certain observers can combine this with other information to create detailed dossiers on individual Internet users. We also show how dangerous this can be - not just to individual privacy, but also to corporations wanting to guard their trade secrets, to any organisation trying to comply with data protection laws, and even to governments trying to protect critical civil infrastructure from attack.

We next lay out the HOPR vision. This is based on a number of core beliefs. Chief among these is that the Internet is a public good - a digital commons that should be safe and secure for all its users. We also believe that it is impossible to provide such privacy using the current Internet infrastructure. What is needed is a new privacy infrastructure on top of the existing Internet. This is what HOPR has built.

The rest of the paper describes on a high level how HOPR works.

HOPR provides a new, privacy-preserving infrastructure for the Internet.

We begin by discussing the HOPR technical solution. This includes the **HOPR network**, a decentralised, incentivised, peer-to-peer network run and maintained by those who use it. Among this network's most important features are that it is public and accessible. HOPR makes it easy even for those without a technical background to participate, either by downloading HOPR's easy-to-use node software, or purchasing a plug-and-play hardware node.

Then there is the **HOPR message layer**. This is the part that provides the privacy. It does so by routing Internet data packets through multiple nodes (a process known as "hopping") and so covering their metadata tracks as they go along their journey. It adds extra security by mixing data packets together, allowing them to lose themselves in the crowd (this why HOPR is referred to as a "mixnet").

Along with this is the **HOPR payment layer**, which makes it possible for HOPR users to

pay the fees necessary to send messages through the network. It also allows HOPR node operators to stake and then earn tokens for successfully relaying traffic.

We then discuss the governance model we have devised for building, maintaining, running and improving this network over time. This model ensures the network is financially self-sustaining as well as fully under the control of its users. Like the technological solution, our governance proposal combines existing approaches with significant innovation. This includes a new form of Decentralized Autonomous Organization (or DAO) that we call DecenGov, short for Decentralised Community-Enabling Governance.

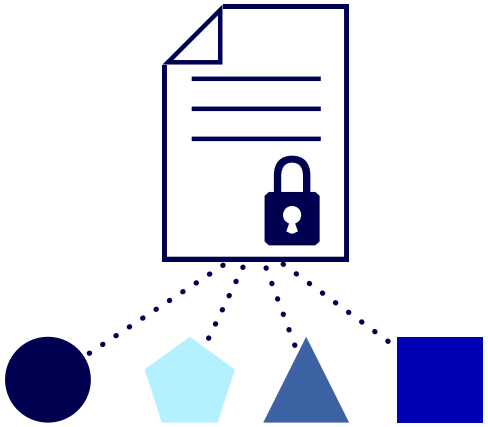
DecenGov-based organisations are legally compliant, protect members from liability, and give members - not a project team or even organisation board - ultimate executive control. DecenGov is the model used by the HOPR Association, the main governing organ of the HOPR network. The Association is open to anyone who holds HOPR tokens and is responsible for all the important governance tasks, from deciding network fees to electing the board, making other personnel decisions and, crucially, deciding how to allocate the network's funds.

We discuss other important details as well, like the HOPR token, and a history of the HOPR project. With all these elements, we hope to paint a picture of what we think this is one of the most important contemporary Internet privacy projects, and encourage all who might be interested to participate.

HOPR will allow everyone - whether individuals, companies or organisations - to use the Internet safely and securely.

PART I: WHY HOPR?

COVERING YOUR CYBER TRACKS: The problem of network-level privacy



While people are increasingly concerned about data privacy online, most are unaware of how the seemingly innocuous metadata used to route Internet traffic exposes them to surveillance. The problem is ubiquitous, dangerous, and - until now - largely unaddressed.

Imagine a world in which everything you did all day, from the time you wake up in the morning through when you go to bed at night, left a permanent record. Where you were, who you spoke to, what you did, what you purchased, what you read, watched or listened to - or even just what you were considering reading, watching or listening to. And now imagine that, like footprints permanently etched in moondust, any observer with the requisite tools and knowledge could read this record at any time and use it to build a real-time dossier of your daily life - all without you knowing a thing about it.

This might sound like an Orwellian nightmare. Yet it is the reality of the Internet today, a result of the fact that almost everything we do online leaves cyber tracks in the form of “metadata” - information about the information we are sending that is visible to anyone with the desire and wherewithal to read it. Not just governments, not just telecom operators or technology companies, but a vast host of private, for-profit entities too.

Such a scenario clearly poses a threat to us all as individual users of the Internet. It is just as worrying for the companies, organisations and, increasingly, machines that rely on the Internet as well. Yet for all the justified public concern about control and abuse of personal data by large platforms, the issue of ubiquitous surveillance of our metadata remains largely off the radar.

At HOPR we aim to change this - both by raising awareness of the problem and, as we describe in this paper, by offering a pragmatic solution to it.

METADATA: THE ACHILLES' HEEL OF ONLINE PRIVACY

First to the problem.

Every time we surf the Internet or send data, for example a chat message, the request needs to include information to ensure it is routed to the correct destination. This is similar to an old-fashioned letter, which needs to be placed in an envelope with a destination address on it and, in case it cannot be delivered, indicate a return address too. For the message to get from A to B, these envelopes have to be easily readable by those responsible for delivering them. It is this address information on the outside of digital envelopes that we refer to as metadata for the purposes of this paper.

Even if they are never opened, these digital envelopes can reveal a shocking amount of information: our IP address, which can often be matched with our name and so reveal who we are; the online services we are using; our entire browsing history; who we are communicating with; when we are communicating; where both we and the receiver of the message are located; how much data we are sending; and more.

That is bad enough. Worse is that these envelopes pass through the hands of a host of different entities who can easily observe them. Some are obvious, like the ISPs, telecom companies and DNS servers needed to make the Internet work. Others are not.

For example, if we visit a website with an embedded YouTube video, then Google, which owns YouTube, will be notified of our visit even if we do not click through to the video. By itself, such a piece of information

is not so revealing. But if we have a Google account, then this information can be linked to our name via our IP address, which Google likely already knows, and added to the detailed dossier that Google maintains on us. This will happen anytime we even tangentially, or inadvertently, interact with Google, providing a constant drip of data points about us that Google can piece together into a full picture. Nor is it just Google. The same thing can happen with a Facebook plugin, or one from a blog-hosting site like Medium. This type of surveillance does not require cookies or any extra code on the part of the observers. It is simply a function of how the Internet works today, there to be exploited by those who know how.

This is not illegal, nor is it a priori bad - but it is certainly more than most people bargained for. The extent of the problem can also be surprising, even to tech-savvy privacy advocates like ourselves. We learned this recently when putting together the privacy policy for the HOPR website.

From the beginning we wanted to make our own website as safe and privacy-preserving for visitors as possible, and we wanted to be as transparent as possible about what happened to the user's personal data. Yet we discovered that if we wanted to also use YouTube to host our videos, or Medium to host our blog, these companies had access to our visitors' metadata and there was nothing we could do about it short of giving up on those services. As a result, we could not guarantee our website visitors that their metadata, including IP address, would not be collected by third parties. It was a sobering lesson for a privacy-oriented project, but also reinforced us in our determination to do something about it.

Of course, this is not a problem just for us. It affects everyone. Combined with other information, metadata like IP addresses can provide the missing link to connect all sorts of disparate pieces of data to specific computers and individual users, and do so on a large scale. This is one reason the Court of Justice of the European Union has said that, under certain circumstances, IP addresses can be considered personal data. It is also why, as Edward Snowden revealed, entities like the NSA consider metadata so valuable they will go to great lengths to collect as much of it as they can.

For most of us, constant surveillance would be a nightmare of Orwellian proportions. Fewer seem aware that this reflects the reality of the Internet today.

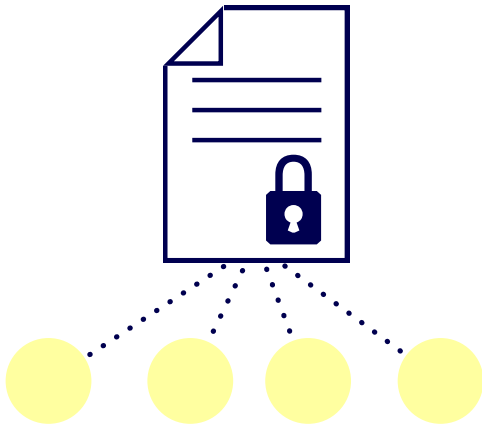
FROM ORWELL TO KAFKA: THE MANY NIGHTMARES OF METADATA SURVEILLANCE

We do not think you have to be a privacy zealot to be frightened by these scenarios. Yet many people underestimate how serious the situation is.

Certainly if you are a journalist exposing corruption, a whistleblower flagging wrongdoing at a major corporation, or a refugee trying to escape imprisonment for your political beliefs, it can be a matter of life and death to ensure your online activity cannot in any way be correlated with who or where you are. But these are exceptional cases.

Imagine instead that you are an ordinary citizen going to the hospital for an examination. Then imagine that there is an observer on the Internet, perhaps your cloud provider

or search engine, who has been collecting your metadata and other digital information about you for a while, and so knows the IP addresses of your devices. By observing you message a taxi from your phone and then half an hour later send text messages from the hospital, this observer would know that you have made this trip. If this observer knows the IP address of an internet-enabled medical device in that hospital room, which is certainly possible, and if that device begins sending data to the hospital's cloud while you are in the room, the observer could reasonably conclude that it is data about you. If the observer further knows that this is a heart-monitoring device, it might note in its dossier on you that you may have a heart problem. If this observer has access to your previous browsing history - again, quite plausible - it might check if you had been searching for information on heart disease recently. If yes, it might now conclude that you definitely do have a heart condition and, depending on what you were searching for, what that condition is.



Most people are unaware that, even if they encrypt their data, metadata still reveals information about them. Lots of information.

Many people say they are not overly concerned about data privacy on the grounds that they have nothing criminal to hide. But do we really want it to be almost common knowledge to privately-owned entities where we are and what we are doing at almost all times, and to come to their own conclusions about things as personal to us as our medical condition?

Nor is surveillance per se the only issue. There is the equally pernicious problem of the potential for error. That might not be you in the hospital but a friend who borrowed your phone. Someone might have incorrectly correlated a device's IP address with its type. And so on. The truth is that the observers who are profiling individuals and companies using these techniques may very well be getting a lot of things wrong. These errors can lead to wrong conclusions about who we are, what we have done, or what someone thinks we intend to do. The result of this could be humorous, or it could be highly dangerous. Either way, being unaware of what these errors are, we are powerless to correct them. For us, the dystopia of metadata-level espionage is therefore not frightening just in an Orwellian and totalitarian way. It is equally frightening in a Kafkaesque way - a nightmare consisting of webs of inaccuracies woven around us by entities that are invisible to us, unapproachable, and unaccountable.

SPY VS SPY: METADATA SURVEILLANCE AND CYBER SECURITY

Personal data privacy is not the only problem, however. Consider the heart patient scenario above from the point of view of the hospital. If it is the hospital's device that has helped the observer uncover

personal data about a patient through correlating it with other data, then the hospital may be exposed to liability under any number of personal and patient data-protection regulations like the GDPR in Europe or HIPAA in the US. This may sound far-fetched now, but the GDPR is for example very clear that any data that can be correlated with other information to reveal personally identifying information is covered by the regulation (which is why, as we saw above, the CJEU considers IP addresses personal data). As the courts and lawyers become more aware of the problem, all companies and organisations serving the public online may find that their inability to protect their visitors' metadata could represent a serious compliance risk.

And it is not only personal data that is at risk. Commercial data is exposed too. Imagine you are the Chief Operating Officer of a global manufacturing company with a highly automated supply chain, and that you depend on hundreds of different IoT devices along that chain to follow the progress and monitor the safety of your products. With the metadata-level surveillance techniques we have outlined, it is perfectly plausible that any number of outsiders could be monitoring your IoT devices as well. They may not have access to the actual information, but just by observing where and when these devices send data, they can learn a great deal about your operations. This could include information about what you are shipping, when you are doing it, to whom, and perhaps even if there have been any issues, like a supply chain bottleneck or the tampering of a shipment.

This is the kind of information that you have likely gone to great lengths to protect. How would you feel to learn that, despite your expensive cyber security

precautions, your operatinal and commercial data is still exposed, and in ways you are powerless to prevent? Now consider the very plausible case that one of the observers in our example is your cloud provider, and that cloud provider in turn also counts your competition as a client. Would you feel comfortable knowing that the only thing protecting your most valuable supply chain secrets is the goodwill and honest business practices of that provider?

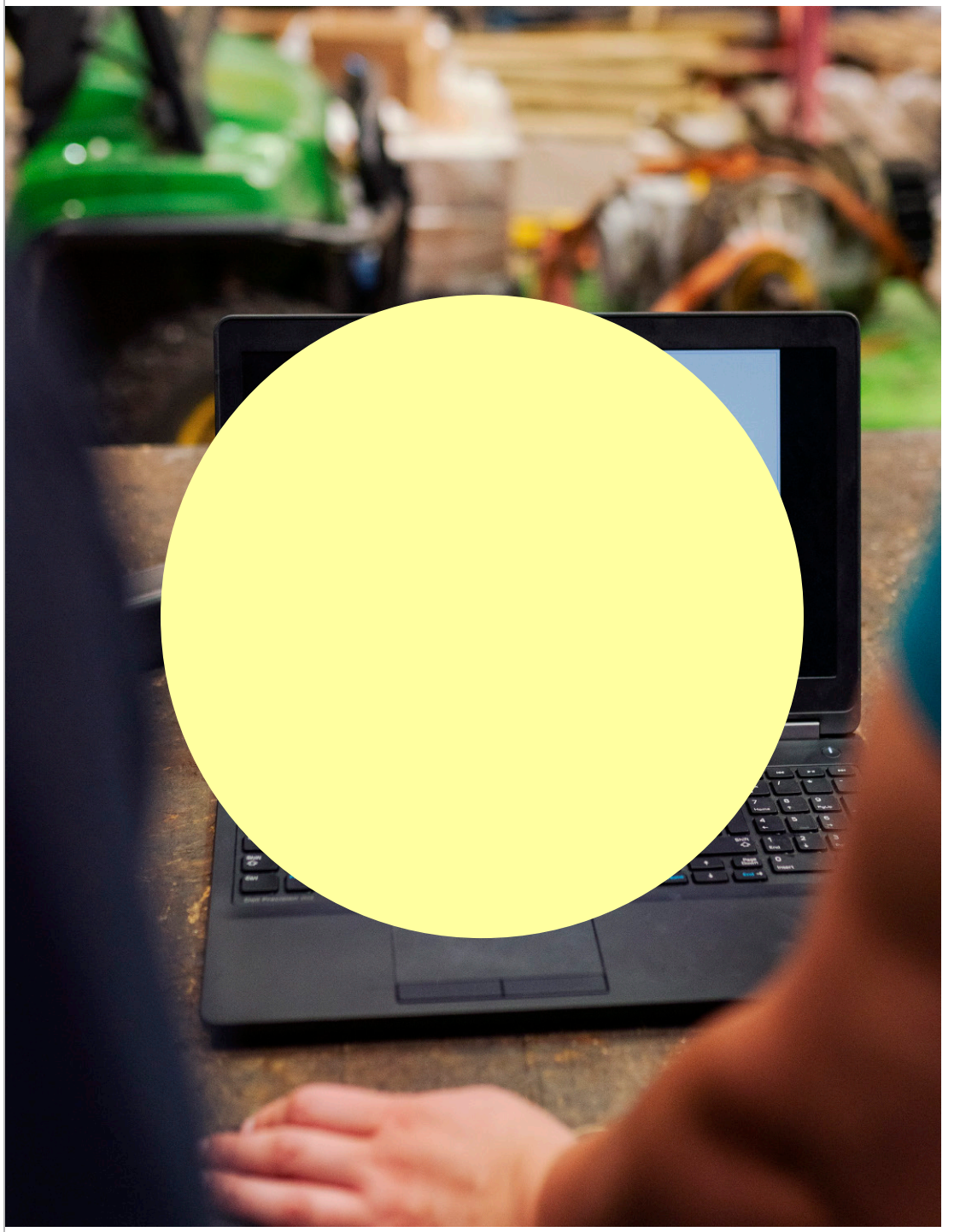
Now consider the case of IoT devices that are part of critical civil infrastructure, for example a city's energy grid. Such infrastructure has become vital to our civilisation, and protecting it is a high priority for law enforcement, officials and planners. What if, despite their precautions, all of the devices in the grid inadvertently reveal how it is designed, how it functions, what its current state is and, potentially, where its weaknesses lie to any observer who knows how to look - including terrorists or other potential adversaries. This is the potential reality if we cannot protect the metadata of our billions of Internet-connected devices.

These scenarios may sound far-fetched, but the technologies to exploit metadata do exist and are becoming ever more sophisticated. In our opinion, this problems needs to be addressed as soon as possible.

You don't have to be a privacy zealot to see how frightenting this situation is.

A PRIVATE, SAFE AND COMPLIANT INTERNET: The HOPR Vision

At HOPR, we believe the Internet is a public good - a digital commons that should be available to all without fear of their activity being recorded by those who have no right to do so. We also believe there is a pragmatic, achievable, community oriented way to accomplish this goal, one that could bring benefits to individuals, companies and society at large.



THE HOPR VISION

Above we saw that, due to the way the Internet functions today, users are exposed to unwarranted levels of surveillance. In this section we discuss our vision of a better way, starting with the set of basic beliefs and principles upon which our vision is based.

Chief among these is the principle that the Internet must be seen as a public good - a digital commons whose primary function is to allow people to communicate and exchange information. Like the mail, the telegraph and telephone before it, it exists for the benefit of its users, not of large platforms or others whose business models depend on gathering and monetising data. We believe that, while there is a legitimate need for certain controls, no one has an unquestioned right to information about an individual's online behavior simply because they have the technical savvy to collect it.

We are hardly alone in this belief. We have seen a sea change in attitudes towards data privacy as well as the data hegemony enjoyed by large platforms. From the Snowden revelations to the popularity of recent books like Surveillance Capitalism and documentaries like The Social Dilemma, public awareness of the problem of data privacy and integrity has increased dramatically. Governments have stepped up to protect personal data in sweeping acts like Europe's GDPR and California's CCPA. And on the technology front, we have seen with the rise of the Web 3.0 movement a number of different initiatives with the common goal of creating an open, decentralised, trustless and above all user-centric Internet.

While we consider ourselves very much a part of this broader movement, we are convinced that it will not be possible to realise Web 3.0

objectives without addressing the problem of metadata privacy. We are also convinced that it will never be possible to provide metadata-level privacy within the current Internet infrastructure. What is needed is a completely new privacy infrastructure to run on top of the current Internet. The good news is that the technology and approaches now exist to build such an infrastructure. We believe strongly that doing so is a reasonable and worthy goal and would be beneficial to all users, whether private individuals, companies, or public sector institutions.

We further believe a privacy-preserving Internet must be built in a transparent way, following free and open source principles and - crucially - that this infrastructure must be built, run, maintained and ultimately controlled by those who use it, not by a private entity or a government agency. Only in this way can we guarantee that it continues to function for the benefit of its users, and is not misused for the benefit of a few.

Last but not least, we believe strongly that success in such an endeavor requires a pragmatic approach. No one can promise perfect privacy, but there are many practical steps that can be taken, and reasonable tradeoffs that can be made, that will result in an infrastructure able to provide far better network-level privacy protection than what is available today. We believe it not only makes sense, but that is essential, to prioritise what is doable over what is theoretically possible but currently unattainable.

We believe that the technology and approaches now exist to add network-level privacy to the Internet, and that building such an infrastructure will be beneficial to all of its users.

TECHNOLOGY AND GOVERNANCE: THE TWO PILLARS OF HOPR

At HOPR, we have a vision for building a privacy-preserving network-level infrastructure that is true to our beliefs and principles, as well as a practical plan for getting it done.

Our vision rests on two main pillars.

On the one hand, we offer a technological solution to network-level privacy that combines existing technologies as well as some cutting edge innovations to create a decentralised, incentivised network run and maintained by those who use it, and which allows those users to communicate, share data and surf the web in an untraceable way.

On the other hand, we propose a governance structure for building, maintaining, running and improving this network over time that ensures the network is financially self-sustaining as well as fully under the control of its users. Like the technological solution, our governance proposal combines existing approaches with significant innovation, including a new form of DAO that is legally compliant, protects DAO members from liability, and gives members - not the project team or even the board - ultimate executive control of the organisation.

Using these ingredients we aim to make the HOPR vision a reality. While we describe the individual parts of HOPR in detail in later sections of this paper as well as in our Technical White Paper, in this section we want to lay out at a high level what HOPR will look like when it is running, and who it will benefit.

The HOPR Hardware Node - just plug it in and partake in the work and rewards of bringing privacy to the Internet.

At the heart of HOPR, there is a global, decentralised network of nodes running the HOPR protocol. The owner of each node earns HOPR tokens for relaying messages. The way HOPR is designed, it is easy for individuals without a technical background to run these nodes and partake in the work and rewards of running the network. They can do this either by downloading software or by purchasing a (mostly) pre-configured hardware node, plugging it in and associating it with a wallet via an easy-to-use app.

In our vision, the majority of these nodes are operated by non-professionals. By this we mean that the network is neither run by a for-profit organisation nor, as is often the case for example with cryptocurrency miners, by those whose primary intention is to profit. Instead, we envision HOPR nodes being run by individuals, small businesses, service organisations, or even corporations whose primary motivation is either a concern for network-level privacy or a desire to use the HOPR network themselves. A node operator who is also a user, for example,

may find that the fees earned for running a node roughly cover the costs of running that node plus the fees for the operator's use of the HOPR network to send messages and safely surf the Internet.

That said, while some - indeed, hopefully many - will be motivated by altruism, we do not think that will be enough to entice a sufficient amount of people to participate. That is why HOPR also provides economic rewards for operating a node. As we describe in more detail below, we consider incentivisation a central part of the HOPR concept. Not only does it catalyse participation. It also aligns self-interest with the interest of the network by making cooperating for the good of the network the only economically viable way to behave. This differentiates HOPR from earlier privacy networks such as Tor, which is not incentivised. This is, in our opinion, one of our main innovations. We also think this is the right path to go for Web 3.0 infrastructure in general, as it will support decentralised applications running at scale in a sustainable fashion.

On top of this network we envision an expanding ecosystem of HOPR-enabled apps, browsers, and other kinds of services that rely on private messaging, as well as an expanding list of app developers and service providers to develop these products and bring them to market.

Behind the scenes, the protocol continues to be developed by the HOPR Association, a member-run organisation based on the new DAO model developed by the HOPR project (see below). The Association, which is open to anyone owning HOPR tokens and who is interested in supporting the goals of the Association, oversees the continued development of the HOPR protocol through its ability to

manage the HOPR token treasury and so issue grants to developers and projects that benefit the ecosystem.

Many different types of individuals and organisations will benefit from the HOPR network and ecosystem. Individuals could use HOPR-enabled browsers run on a subscription model, akin to today's VPN software, to allow them to surf the Internet in a safe way, knowing they are not being profiled. They could also use HOPR-enabled chat platforms for highly secure messaging. Hospitals could use HOPR-enabled IoT platforms to ensure that their connected medical devices can communicate securely with one another, protecting patient privacy and reducing the complexity and cost of regulatory compliance. Banks could use HOPR-enabled data exchange to interact securely with blockchains, helping ensure financial services grade privacy for their ever-expanding cryptocurrency clientele.

At the heart of HOPR is a global, decentralised network of nodes running the HOPR protocol, an ecosystem of dApps and services built on top of it, and a community of node operators who keep the network running and earn HOPR tokens for their effort.

ABOUT THE HOPR PROJECT

HOPR is a Swiss-based project started by an experienced team of cryptographers and blockchain experts. Both the HOPR project and ecosystem have grown dramatically over the project's first two years, auguring well for its future.

The HOPR team is based in Zurich, but international in nature, and growing all the time.

Technology projects are as much about the people involved as they are about the technology itself or how it is used. In this section we provide a short history of HOPR and the team behind it, as well as discuss its early backers and the growing community of HOPR enthusiasts who have been putting the technology through its paces during various test phases, and so helping to refine it.

PRE-HISTORY OF HOPR

The HOPR project traces its roots back to early 2018. Members of what would become the core team, then part of a blockchain consultancy headquartered in Zug in the heart of Switzerland's Crypto Valley, were approached about building a decentralised app for a use case that among other things required absolutely secure direct messaging between individual users. While the original project was cancelled after the bursting of the crypto bubble in the Spring of 2018, the core team remained intrigued by the problem of network-level privacy – a problem, the team soon learned, that interested a great many people in the blockchain and Web 3.0 development and academic communities, but which had yet to be solved. Increasingly convinced of the importance of network-level security, the team took the decision at the end of 2018 to formally found HOPR with the purpose of finding a workable solution.

Early work was mostly theoretical, with the project team taking a deep dive into the technical challenges, evaluating the strengths and weaknesses of existing solutions, and sketching out their high-level vision and architecture for the new technology. The team also began implementing early versions of the protocol, and by Q1 2019 was ready to show it to the world, if only in a very early version.

TAKEOFF: A FIRST LOOK AT, AND FIRST INTEREST IN, HOPR

The team held the first-ever demo of the HOPR protocol at the EthCC conference in Paris in February 2019. From that point on, interest in HOPR began to grow dramatically. Among other things, the demo caught the eye of members of Binance, the world's largest cryptocurrency exchange, who were attending the conference. This led to a Binance Fellowship grant for one of HOPR's co-founders. HOPR also received a grant from the Web3 Foundation, which was interested in its work on network-level privacy as well. Significantly, the team was also approached by a medical device company in need of network level security for its IoT senses. This was a welcome early validation of one of HOPR's main use cases.

In 2020 things really took off. Binance led a seed round of USD 1 million, and announced that it was highly committed to the project. After this both the HOPR Association, the DAO that will ultimately run the HOPR network, as well as HOPR Services AG, a for-profit entity founded by the project team to work on the early stage development of the project, were founded.

During this year HOPR also began releasing testnets at a fast pace, each one named after a famous Swiss mountain, and featuring a more mature, though still early, version of the protocol. While all testnets were made available as a software download, the project also released its HOPR Hardware Node PC during the year. This was an important milestone on the way towards a simple, user-friendly way for any individual to take part in HOPR.

To help catalyse interest in running test nodes, as well as sufficient network traffic

to carry out the tests, the testing process was gamified, with users able to earn HOPR tokens for taking part, carrying out tasks, solving puzzles, and the like. The approach proved successful, and interest in these testnets grew rapidly in the community and beyond. By the end of the year there were over 1,000 people around the world running HOPR test nodes and actively interacting with the project, uncovering bugs, and offering their suggestions. The wider HOPR community also experienced exponential growth. As of this writing, the HOPR Telegram channel for example has grown to over 6,000 users. It now supports multiple languages including English, Mandarin, Russian, Spanish, Portuguese, Vietnamese, Korean, Japanese, and Indonesian.

LOOKING AHEAD: THE HOPR ROADMAP

Having accomplished a lot in two years, the HOPR project found itself at the end of 2020 planning to go live. The Roadmap includes an initial launch of the HOPR Mainnet not containing cover traffic at the end of January. This will be followed by a full Mainnet Launch including cover traffic in February. With this the HOPR network will be both live and feature complete.

After this, the project will turn its attention to the broader HOPR ecosystem. In a first step, it intends to officially open up the HOPR Association in May to a larger number of members. This will be the DAO, built on HOPR's new DecenGov framework, through which the HOPR community will govern the network. In May, the project will release its first API, enabling others to develop metadata-private dApps and services on top of the HOPR protocol. This move will catalyse the growth of the larger HOPR ecosystem. Finally, in September of 2021

the HOPR Association intends to hold its first General Assembly. All holders of HOPR tokens will be eligible to become a member in the HOPR Association and vote in the Assembly, marking the point at which HOPR becomes completely independent and self-sustaining.

These are ambitious plans. And while progress as of this writing would indicate that these milestones are attainable, the plans could be subject to change. For up-to-date details on planning and progress, the interested reader should consult the HOPR website.

The HOPR project accomplished a lot in its first two years. In 2021, it will be going live with both its technology and innovative governance approach.

Nov 2018 — **Idea**
HOPR's founders develop a decentralized approach to the urgent issue of metadata privacy. HOPR is born!

Apr 2020 — **Funding and Launch**
HOPR officially launches, concluding a $1m seed funding round led by Binance. The HOPR Association is founded.

Jul 2020 — **Hardware Node**
The HOPR Hardware Node launches, allowing users to run a dedicated HOPR device from their home.

Nov 2020 — **Testing and Community**
A series of popular incentivized and gamified testnets grow the community and network to over 2000 nodes.

Q1 2021 — **Jungfrau Release**
The HOPR Jungfrau release is the first feature complete version of the HOPR node & HOPR token.

Q2 2021 — **Eiger Release**
HOPR's Eiger release introduces cover traffic and provides increased incentives for relay node operators.

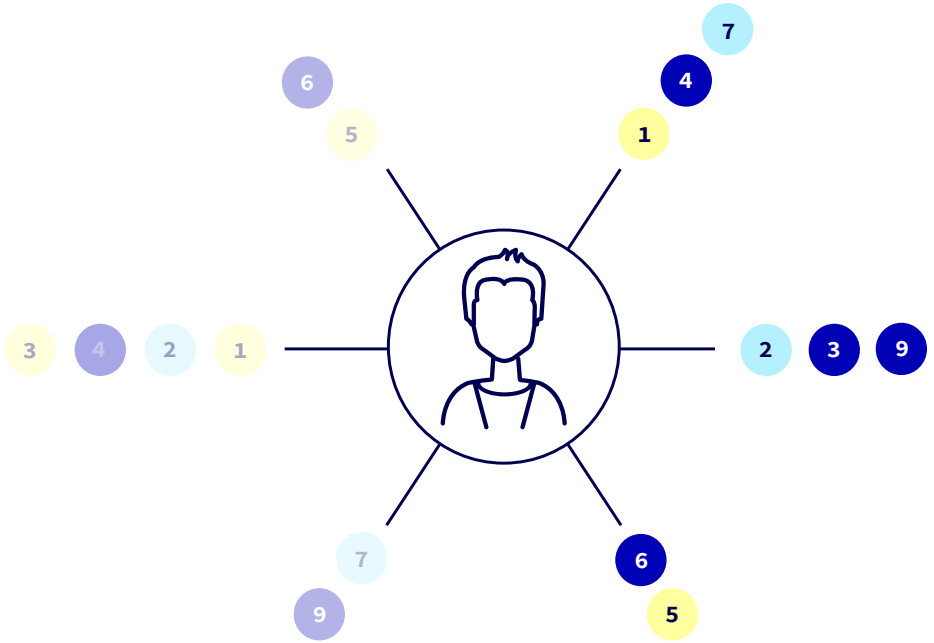
Launch DAO
HOPR's focus on decentralized community enabling governance is solidified with the launch of a DAO.

Launch of Ecosystem
A robust API allows others to build metadata-private dApps and services on top of the HOPR protocol.

Q4 2021 — **Token-based Voting**
All token holders will be eligible to vote in the first General Assembly of the HOPR Association.

PART II:
How HOPR works

HOPR TECHNOLOGY



The HOPR network is designed to provide network-level privacy both by the use of a messaging protocol that obscures metadata so that individual data packets do not reveal trackable information, and a decentralised network that is managed by its users, so that there is no danger of a controlling entity abusing its power. To compensate individuals for the work of running a node, HOPR also contains a native currency and incentivisation scheme.

In this section we lay out, in non-technical terms, how the HOPR network is designed and how it works. For technical details and a more in-depth view, readers should consult our forthcoming technical white paper, which will be made available on the HOPR website.

While the technical architecture is fairly complex, the HOPR protocol can be best understood as a protocol that enables a public, decentralised, peer-to-peer network on top of which two main layers run: a message layer and a payment layer.

THE HOPR DECENTRALISED NETWORK

The HOPR network is a decentralised, peer-to-peer network open to anyone who wants to join and run a node. Its design is meant to support the key elements of the HOPR vision.

Because it is decentralised, there is no entity that controls it. No one with special administrator rights, no master node or server to control traffic or access. Instead, all the nodes are peers that, through the simple expedient of running the HOPR protocol, work together to run the network in communal fashion. Decentralisation ensures that the network is independent, with no one in a position to unduly influence its development or manipulate outcomes to their advantage. (Not even members of the HOPR Association, who are tasked with managing the network, can control, censor or intercept its traffic.) It also makes the network resilient, able to keep running even if a majority of nodes are damaged or compromised and very difficult, if not impossible, to shut down.

The network is also public. The only requirement to become part of it is to run the

latest version of the HOPR protocol. Our goal is to have as broad a base of node operators as possible. For this reason, HOPR nodes are designed to be easy to set up even for those without a technical background. Anyone who wants to be a node operator can either download the software and run it on their computer (or on a virtual server in the cloud). Or they can purchase a HOPR Hardware Node and plug it in to their Internet connection at home. After a simple configuration process via a browser or phone app, the protocol then runs by itself on the node - offering a convenient, plug-and-play way to take part.

The setup procedure will also enable a node to receive and hold tokens. In order to participate in the network, each operator will need to acquire HOPR tokens, generally from an exchange, and then "stake" them in payment channels. The more HOPR tokens that are staked, the more traffic the particular node can relay, and therefore the better chance the node has of receiving payment. The protocol software makes the staking process relatively easy. Users however will have to decide how many tokens they want to seed the node with, understanding that the revenue generated by the node is proportional to the amount of HOPR tokens staked. (You can find more on payment channels and HOPR incentivisation in the respective sections below.)

Anyone wanting to use the HOPR network to send messages or data will need to acquire HOPR tokens as well. These are used to pay the network fees, which are charged per use in micro-units of the token. These fees are then used to pay the node operators for relaying traffic, as described above. (The mechanism for this is also described in more detail in the relevant sections below.)

THE HOPR MESSAGE LAYER

The message layer of the HOPR protocol is designed to solve the problem of how to send a message - or, to be more technically precise, a "data packet" - from one point in a network to another without revealing from where, from whom or when the packet was sent, or where it is going. This is tricky, analogous to posting a letter without a to or from address and no stamp, and expecting it to be delivered to the right place on time.

HOPR solves this problem by not sending packets directly from point A to B, but rather through a series of intermediate steps that can be described as from A to receiver Z by way of nodes B, C and D. This process is known as hopping, and gives HOPR its name.

Metadata-privacy is achieved by the fact that the protocol routes the messages in such a way that the intermediate nodes only know the immediately adjacent nodes. When A sends the packet to B, B knows that the packet came from A (though - crucially - not the fact that A is the originator of the message), and that the packet has to be forwarded to C. B however does not and cannot know that the ultimate destination is Z. Similarly, C sees that the packet has arrived from B and needs to be forwarded to D, but knows nothing of A. When D forwards to Z, the protocol also hides the fact that Z is the final destination. Thanks to this approach, known as onion routing (the technology behind Tor), the packet's tracks are slowly but surely covered up as it makes its way toward its desination. Similarly, no one along the chain can ever have the full overview of what traffic is going where.

While onion routing goes a long way to protecting metadata, by itself it is not enough.

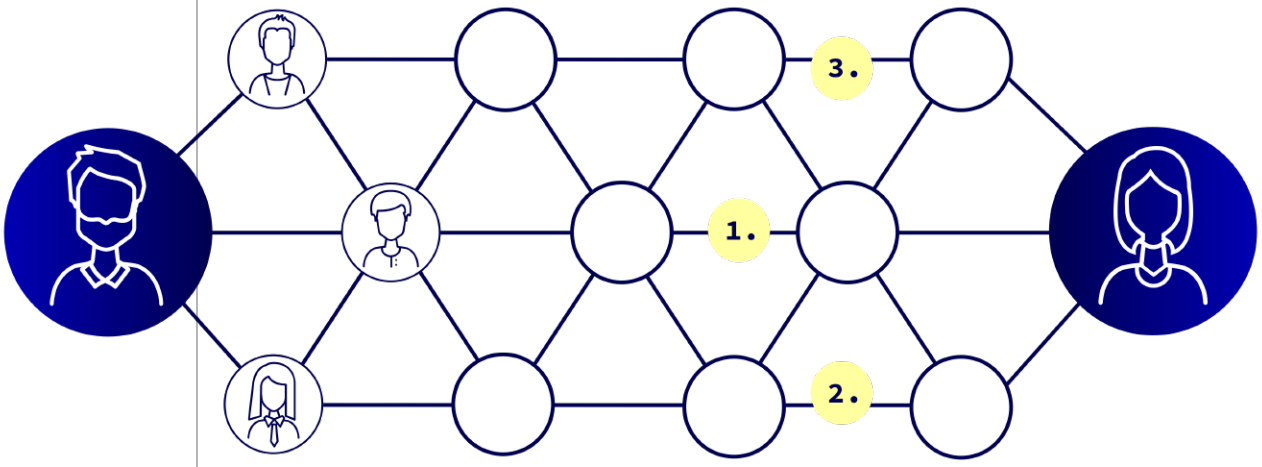
Meta-information can still leak, revealing for example the size of the message, or information that can be used to link the outgoing packets from sender A with incoming packets on receiver Z's end.

For extra security, HOPR therefore also employs packet mixing. In this approach, messages travelling through a node are not immediately forwarded but rather cached for a short amount of time and then mixed together with other packets that were received around the same time. This is done in such a way that the packets in effect get lost in the crowd. Thanks to the Sphinx packet format that HOPR uses, packets are also transformed such that outgoing packets cannot be linked to incoming ones. In addition, the Sphinx format also ensures that necessary metadata in the packet header, such as the address of the next downstream node to receive the packet, are not revealed to an observer. Thanks to this approach, to an outside observer all the traffic running through the HOPR network looks like one big, inscrutable jumble of bits and bytes. Under the cover of this jumble, packets can make their way safely back and forth.

Mixing can only work if there is sufficient traffic on the network. It is like an 80,000 seat football stadium in which it is relatively easy to pick out a single person if there are only 500 people present, but almost impossible if the stadium is full.

Since network volumes can vary over time, the HOPR protocol needs to ensure that there is always enough traffic to provide privacy. It therefore also generates a constant stream of arbitrary data packets known as "cover traffic". This creates sufficient message cover (hence the name) to hide the legitimate messages. It also has the important side effect of providing a constant

stream of work for the nodes, ensuring there are sufficient revenue opportunities to keep it economically viable to be a node operator.



HOPR gets its name from the fact that it provides metadata privacy by sending data packets through multiple nodes - or "hops" - in the network.

As with any security mechanism, HOPR's network-level privacy involves some tradeoffs. With regard to the HOPR message layer, there are two main issues users should be aware of.

First is the question of speed. The use of the multihop routing scheme and the mixnet slows down packet delivery, adding latency to the network. For this reason users on the HOPR network can choose the level of security they want, from 0 hops and no mixing, which still provides some basic privacy via the Sphinx packet format that HOPR uses, to three or more hops and long-latency mixing, which provides maximum privacy.

Second is the issue of potentially reduced privacy due to the way HOPR generates cover traffic. The issue is this: In order to work smoothly, the amount of cover traffic needs to be adjusted to fit the actual network volumes. As currently conceived, the HOPR Association will be solely responsible for

sending cover traffic and tuning its volumes as needed. This is a centralised solution, and so a limitation of the first version of HOPR. Subsequent versions will implement decentralized and cheat-proof cover traffic allocation. The initial version therefore represents a temporary compromise, but one we feel is fully in line with our stated goal of taking a pragmatic approach.

THE HOPR PAYMENT LAYER

The problem that the HOPR payment layer solves is how to reward node operators for forwarding data packets without inadvertently revealing metadata about those packets and so defeating the purpose of the network. This has long been recognised as a serious problem in trying to introduce incentivisation for a mixnet, and there are those in the academic community who argue that it is impossible to create a completely private/anonymous payment scheme for an incentivised mixnet.

Here, too, we are very aware of the theoretical, though by no means insignificant, risks involved. From the outset we have however believed strongly that you cannot have true network-level privacy without a decentralised network, that you cannot have a truly decentralised network without a decentralised means to reward node operators for relaying messages, and that it is possible to devise an approach that mitigates the risks to a more than acceptable degree.

This latter we have accomplished with the HOPR payment layer. We consider this to be perhaps our most important innovation - a pragmatic solution that can be implemented in the real world that, while not perfect (and no one can or should ever claim to offer perfect security on a digital network) functions very, very well.

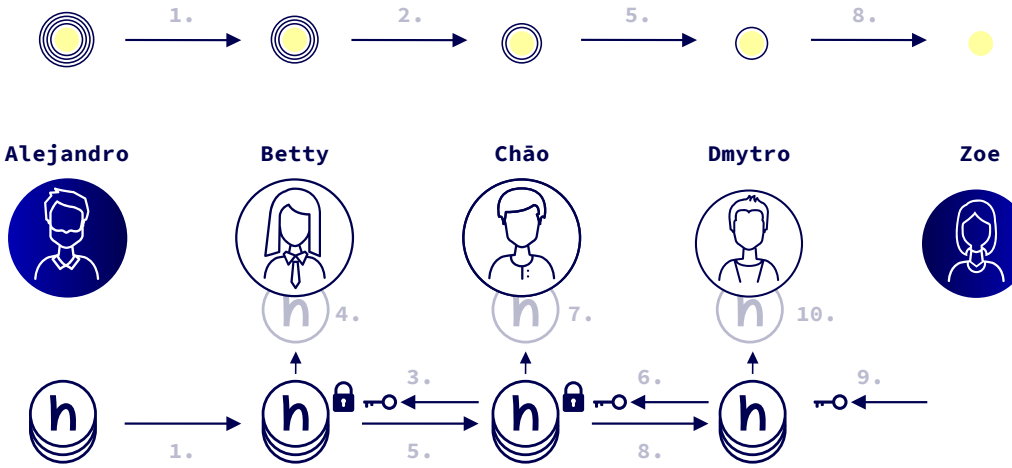
The details of the payment layer are complex, but at the heart of it lies our proof-of-relay scheme. On a high level it can be understood as follows: Every time a node operator forwards a packet they earn the right to receive a payment. Relayers, however, only receive half the information they need to try and claim a reward when they receive the packet. They are given the other half when they have successfully forwarded the packet to the next node on the journey.

It is important to understand that matching payment key pairs in HOPR do not automatically result in a payment. Rather they are like a lottery ticket that gives the holder the right to be chosen for a payment. This is an added security feature, as this lottery helps de-link the payments from the underlying packets. The protocol is designed in such a way that all nodes have the same chances of winning and that, over time, rewards will be roughly proportional to the stake of a participant. That is why the HOPR payment channels are also referred to as **probabilistic** micropayment channels.

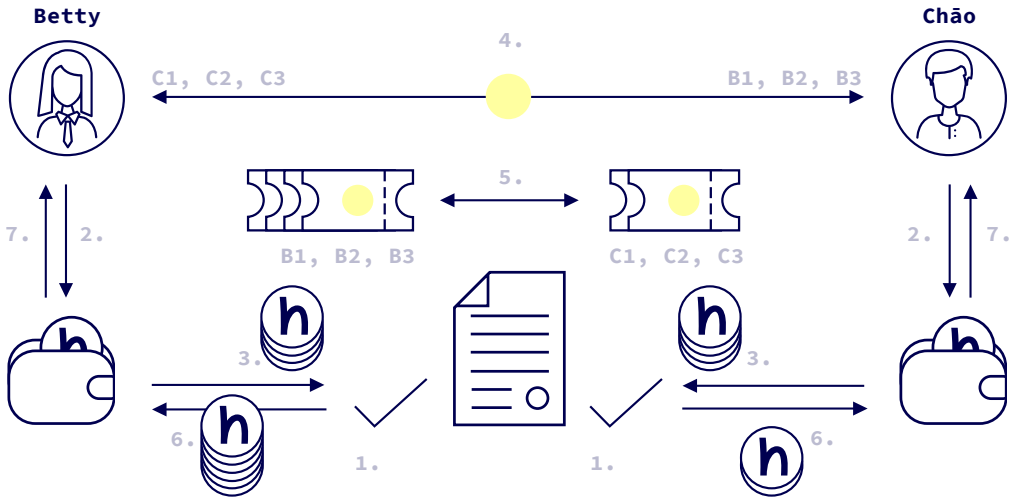
This provides security in a number of ways. Firstly, since the two halves of a payment key are useless on their own, the only way to get rewarded is to properly forward a packet. As there is nothing to be gained from trying to cheat the system, the self-interested way to behave is to cooperate by adhering to the protocol. Secondly, by separating out the payment layer, proof-of-relay ensures that there is no connection between the payments and the underlying data packets. This prevents inadvertent data leakage.

Finally, as mentioned above, node operators need to stake HOPR tokens to fund payment channels between their nodes and peer nodes in order to relay data. This is important as the only way to economically settle the kinds of high volume micropayments found in the HOPR network is to lock-up collateral in a payment channel. Staking also has some beneficial side effects. Because it represents economic value at risk, it incentivises node operators to only “do business” with well behaving nodes, and so adds a self-policing aspect to the network. Staking also means that a large number of HOPR tokens will be out of circulation at any one time, reducing effective supply.

In terms of the HOPR network, incentivisation is a deliberate design choice. It helps ensure resiliency of the network by making it economically worthwhile for large numbers of individuals to run nodes. This should also help the network scale, ensuring it can handle heavy volumes of traffic. Because fees are distributed equitably to all nodes who participate, it ensures that the economic benefits of the network don’t accrue to a small number of entities. This safeguards decentralisation.



HOPR provides network level privacy through a process known as ‘onion routing’. As a data packet hops from node A to B to C to D and ultimately to Z, the packet’s metadata tracks are slowly but surely covered up. With HOPR’s innovative payment channel, nodes who sucessfully relay traffic receive a ‘proof-of-relay’ key. Combined with the right key from adjacent nodes, it can be used to earn HOPR token rewards.



When node operators receive a data packet to forward on, they only receive half the information they need to claim the reward for the work. They receive the other half when they have succesfully forwarded the packet to the next node on the journey.

HOPR GOVERNANCE

HOPR is not only a decentralised network. It will also become a decentralised, global, community-run organisation. The HOPR Association, which employs a new, legally sound and truly transparent DAO approach called DecenGov, will ensure that the HOPR network is run by and for its users.

THE NEED FOR DECENTRALISED GOVERNANCE

When we started HOPR, we quickly realised that the only way we could assure network-level metadata privacy over the long haul was by means of a decentralised network – that is, a network that ran autonomously on its own without any controlling company or organisation.

If this was not the case – if there was someone with administrator rights, or a for-profit (or even non-profit) organisation with ultimate say – then there would be too much risk of those in control somehow abusing or misusing their power. For many use cases, of course, outsourcing trust, even to a limited degree, to a central authority of some kind makes sense. But in our opinion, there is too much at stake in a privacy project like ours to take that risk. A network like HOPR must be governed in a trustless way, run and managed by those who use it. So to us, decentralised governance is not just an idealistic goal (though we are strong believers in decentralisation). It is very much an integral part of the technological design: without it, the network could not function.

That said, decentralised governance can be challenging. Since we come out of the blockchain world, we have naturally been influenced by blockchain and cryptocurrency projects, many of which employ either formal or informal decentralised governance models, or some combination of both. But while decentralised governance is very difficult to implement without blockchains to act as trust layers, the track record of decentralised governance in the blockchain world to date has been mixed to say the least.

Bitcoin, to name the most prominent example,

has indeed survived and even thrived for over a decade with no formal governance structures, though not without its governance crises, controversies, and schisms. As an open source project with no legal entity (or identifiable founder), it is also unclear who bears liability should something go wrong. In the worst case, this could be any or all who have contributed to the code. Another example is the Tezos project, which was designed specifically as a “governance” blockchain protocol under community management. It stumbled famously in its early days because too much power had been inadvertently given to the Foundation that had been set up to oversee it.

The truth is, while decentralised governance is extremely important in our eyes, we also know that achieving it is very difficult. Among other things, finding the right balance between the need for executive decision-making capabilities with the need to give everyone involved in a decentralised endeavor equal voice, is extremely tricky. For this reason we have put as much thought and effort into designing our governance model as we have into our technical solution.

The only way we can assure network-level metadata privacy over the long haul is by means of a decentralised network - a network that runs autonomously on its own, managed by its users, and not under the control of any company or organisation.

INTRODUCING DECENGOV

When it came to governance, as a Swiss-based project we had an advantage considering that many of the major innovations in decentralised blockchain governance originated in the Swiss crypto community.

The Ethereum Foundation, the first consciously designed decentralised blockchain governance organ, was founded in Zug in 2015. It in turn was based on the tried and true principles of Swiss Foundation law. This was found to be quite conducive to blockchain projects and initial coin offerings (ICOs), as it gave those projects legal standing while in theory providing token buyers and token holders assurances that the non-profit Foundation would act solely on their behalf. As Tezos, among others, demonstrated, this was not without its flaws. As it turns out, under Swiss Foundation law projects token holders remained largely excluded from executive decision, and projects remained overly exposed to the whims and follies of Foundation boards and/or project teams.

We wanted to do this one better, and were lucky to discover the answer here in Switzerland as well. Working with FRORIEP, one of Switzerland’s leading crypto law firms, we have developed a brand new, decentralised governance mode we call Decentralised Community-Enabling Governance, or DecenGov for short.

DecenGov provides token holders not only legal certainty and liability protection, but also protects projects from being taken over by internal groups. Its main innovation is that it is based on Swiss Association law, not Swiss Foundation law. The differences are subtle, but significant. Swiss Association law is very flexible in terms

of governance structures. Under its legal cover, we were able to design DecenGov to ensure that token holders have a real say, not just in the technical development of a platform but in the executive decisions of the project. We could also ensure that token holders always had the last word. Yes, there is a Board, but the real power lies within the General Assembly of members.

The goal of DecenGov is to achieve the right balance between on-chain and off-chain governance. On the on-chain side, it puts the ultimate decision-making power with the community of token holders, with each token representing a single vote, though with an important twist. To ensure the Association does not become an oligarchy dominated by large token holders, we employ quadratic voting, a new democratic voting scheme that has found early applications in the Colorado state legislature as well as blockchain projects such as Gitcoin. In quadratic voting, the voting power of each party is proportional to the square root of tokens that are held by a party at the cutoff time for the vote or general assembly. The more someone wants to vote for a measure, the more expensive it becomes. This has been shown to even the playing field between large single holders of tokens and large groups of small token holders.

On the off-chain side, the HOPR Association is a recognised legal entity in Switzerland. Crucially, it also protects individual members from liability, an issue that plagues decentralised governance structures that do not have sufficient legal grounding.

THE HOPR ASSOCIATION AND WHAT IT DOES

DecenGov is a framework. We consider it a major innovation in the area of Decentralised Autonomous Organisations or DAOs, to be used by all who are looking for an advanced model to ensure a fair and robust decentralised governance.

The HOPR Association, in turn, is our implementation of the DecenGov principles for the HOPR Community. Founded in Zurich in March of 2020, membership in the Association is currently open to anyone who can demonstrate ownership of HOPR tokens and who is approved by the Association Board. Since as of this writing HOPR is not yet live, the Association Board is made up of members of the HOPR team. But this is only for now. At the first General Assembly, currently scheduled for end of 2021, the Association will be turned over fully to HOPR token holders.

The members of the Association will have a number of specific and more general governance tasks.

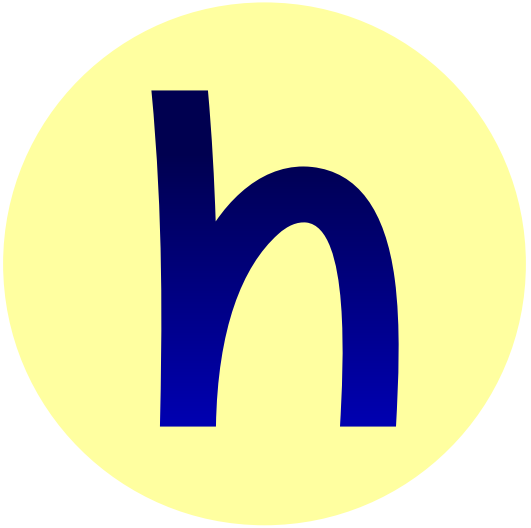
Specific to the HOPR network, the Association has to decide on the initial network fees and the rewards for network relayers until the HOPR DAO is ready to take over. These need to be set in such a way that they strike a balance between providing sufficient earnings potential to relayers, thus ensuring sufficient incentive to run a node, while keeping the fees for sending messages low, thus ensuring incentive for people to use the network.

More generally, the Association's General Assembly will be tasked with growing and supporting the network over time. This includes personnel decisions, from electing Board members to potentially making decisions

on hiring Association staff or outsourcing some aspects of running the Association to third parties. It will also include the all-important question of how to spend the Association's funds. Where those funds come from, and to what extent the Association will have control over them, is described - along with much else - in the next and final section of this paper.

DecenGov is a major innovation in the area of Decentralised Autonomous Organisations or DAOs. The HOPR Association, run on DecenGov principles, will ensure user control of all aspects of HOPR.

THE HOPR TOKEN



As the means of paying network fees, compensating node operators, and enabling participation in network governance, the HOPR token plays an essential role in almost every aspect of the HOPR network and HOPR community. In this section we provide our rationale for having a HOPR token as well as an overview of how the token is designed and will be employed.

ON INCENTIVISATION IN HOPR

While the HOPR network is being designed to be easy to use by anyone simply by downloading software or purchasing a small piece of hardware, there is still work and expense involved. People do have to set up their nodes. They have to keep them running and ensure they are updated. They have to pay for the electricity involved. They have to add this to the list of many things they need to deal with in their lives. Why would anyone do this?

There are two answers. One is altruistic: by running a HOPR node a person can contribute meaningfully to promoting data privacy in the world. The other is more practical, and we think more powerful: in HOPR, the network also offers individuals and entities the chance to earn money for running a node.

This incentivisation is an important element of the HOPR design, and one we think will be a key element of its success for a number of reasons. By incentivising users, HOPR will lower the barrier to adoption. While the idea is not that running a HOPR node will make a node operator rich, the expectation is that doing so will not only pay for itself but, as the network grows, will likely generate some passive income. This in turn could be used to pay network fees, allowing node operators to use the HOPR network in effect for free. This will likely make it much easier for many people to decide to go through the initial effort of setting up a node.

Incentivisation also encourages good behavior – or beneficial coordination – on the part of node operators. As we mentioned above, within the way the protocol is designed, the only way to earn token rewards is to

successfully relay data packets. Since no other behavior is economically rewarding, the only rational thing to do is follow the protocol.

Last but not least, and also as touched on above, because node operators are required to stake tokens in their nodes in order to participate, there will always be a large amount of HOPR capital locked up. This will reduce the velocity of HOPR in circulation.

WHAT THE HOPR TOKEN DOES

The HOPR token itself is a blockchain-based crypto-token that lives on the Ethereum blockchain and conforms to the Ethereum ERC20 token standard – by far the most widely used and interoperable standard for creating crypto tokens.

The token has three main functions, which are described below.

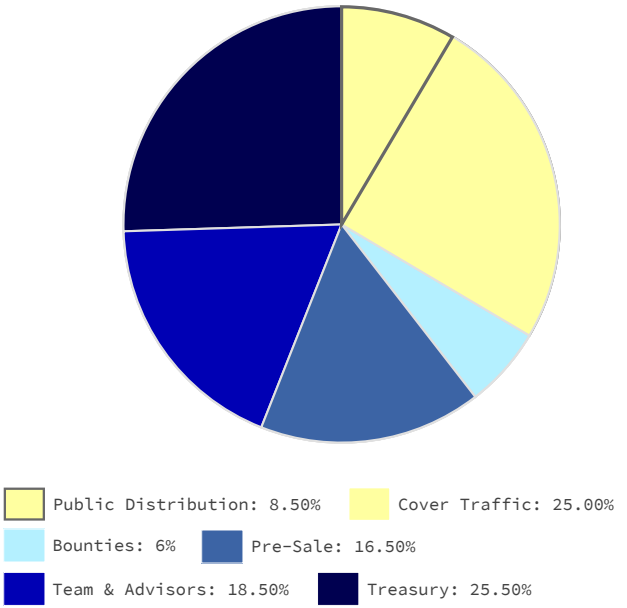
Payment. HOPR tokens are used by senders of a message to pay relay node operators. For each successfully relayed packet, the downstream node reveals a key to the upstream relayer and thus provides a proof-of-relay for that upstream node, as described above. With this key the relayer earns the chance of a payout. This probabilistic micropayment mechanism is similar to obtaining a lottery ticket that - in case of a win - can be redeamed on-chain for HOPR tokens, claimed out of the corresponding payment channel. The expectation value per packet is thus the product of the payout amount (in HOPR tokens) times the odds. Both values (payout and odds) will be fixed prior to the deployment of the mainnet but will be dynamically updateable by token vote after year one. Since requiring end-consumers, for example in a HOPR-enabled private chat application, to pay for sending messages might be a hurdle to adoption, HOPR payment channels allow third parties to provide tokens to their users. A decentralised HOPR chat app might run on a subscription model, like a VPN, and part of the user's monthly fee would go to filling the user's account with the requisite tokens to run the app.

Work and Stake. HOPR relay node operators stake HOPR tokens in dedicated HOPR payment channels in order to be eligible to send data packets or relaying other users' data packets. Node operators open payment channels to downstream nodes and are then able to relay packets through that node. A relay node operator is thereby incentivized to open many payment channels in order to maximize their likelihood of relaying traffic. At the same time, staking HOPR tokens is locking up capital and thus incentivizes node operators to maintain payment channels with active and well-behaving nodes. In addition to signaling availability as a relay node operator, staking HOPR tokens in payment channels entitles the node to relay cover traffic and earn HOPR tokens for doing so.

Governance. As described in the previous section, the HOPR token also entitles its owners to partake in governance of the HOPR network by giving them voting rights in the HOPR Association. The number of tokens held at the time of voting for any proposal confers a right to vote. Token holders do not need to actually spend their tokens to exercise their franchise. As the means of paying network fees, compensating node operators, and enabling participation in network governance, the HOPR token plays an essential role in almost every aspect of the HOPR network and HOPR community.

TOKEN SUPPLY AND RELEASE SCHEDULE

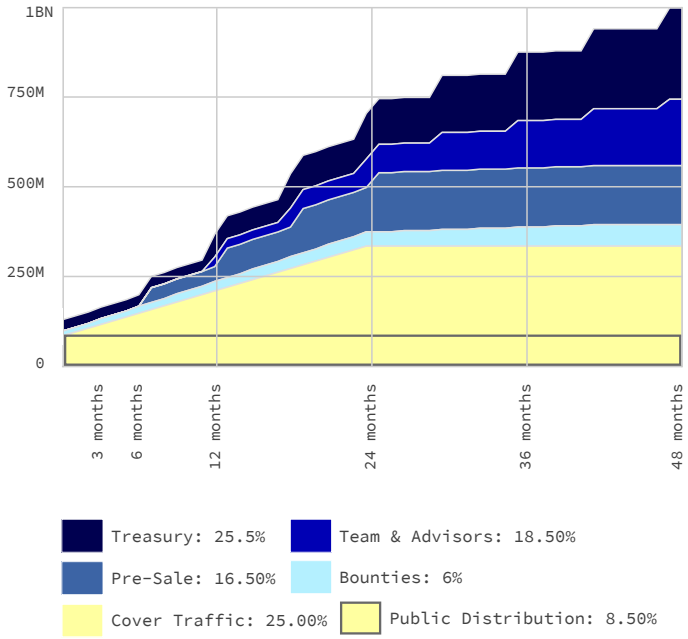
HOPR has a total supply of 1 billion tokens, broken down into the following categories:



One billion HOPR may seem like a lot of tokens, but the circulating supply will be much lower.

First, the stake function (explained above) provides strong incentives for HOPR to be locked.

Second, many of the token allocation categories are set to release gradually over a period of four years, as shown in the chart below.



At launch, the actual circulating supply will be 130m HOPR, and we expect much of that to be locked through staking.

CHANGING DATA PRIVACY FOR GOOD

hopr

AFTERWORD

In this paper we have tried to paint a high level but hopefully easily understandable and compelling picture of HOPR. As we have said, we think the use case of metadata privacy is a very important one, and one that has not received the attention that it deserves. By addressing it, we hope to be able to contribute an important element to what is a much larger movement around the world in favor of greater privacy and data protection in cyberspace - one that counts not just privacy advocates, but governments, regulators, corporate executives and hosts of regular people among its ranks.

While we see ourselves as very much part of this movement, and consider ourselves strong privacy advocates, we have consciously designed HOPR to be idealistic in its goals, but very practical in its approach. HOPR is meant to protect everyone, and to be used by everyone. It is also meant to benefit all who are involved with it. By choosing to build an incentivised network, we have chosen to appeal to every man and every woman, and to encourage them to participate. By making our nodes easy to operate at home, we are enabling them to do so.

This aspect is very important. We have done everything we can to make HOPR as powerful, easy-to-use and effective as possible. But we have also been pragmatic about it, putting a priority on designing something that can actually be built, and making something that people can actually use.

We invite all those who may be interested to do just that: join HOPR, participate in the project, and see for yourself. As our project goes live after two years of hard work to get it on its feet, it really is just the beginning. It is now, as we slowly turn it over to the community, that it will really begin to make its impact felt.

Visit us:
HOPRNET.org