p2p IM & Toolbox – Whitepaper

Index

1. Background

Since 2010, the Instant Messenger (IM) platform WhatsApp has shown exponential growth in active users, from 10 million monthly active users in 2010 to 2.7 billion in 2023. This shows a clear trend that IMs have become the default app for the vast majority of mobile users. In recent years we have observed user bases grow on platforms like Telegram and Signal, mainly based on users' privacy concerns using applications like Messenger and WhatsApp. Active users engage with their contacts directly, or within public and private groups, where the user profiles and messages are recovered from a centralised server (presenting privacy concerns).

Over the past 5+ years, we have witnessed a growth in users paying for subscriptions to follow content creators, who produce regular content for their communities. Users will also pay additionally for extra engagement within the live chats, where messages are made more prominent and they may receive a shout-out (as an example). Depending on the platform users may place on a leaderboard, based on their level of interaction within the community and money donated to the creator channel.

Platforms, for example Twitch, that host these communities will take anywhere from 20% - 30%+ in fees, on any funds that are sent from users. Also, users who follow creators online, do not receive anything tangible or meaningful that represents the communities they engage with and actively contribute. They may fall on a leaderboard or receive channel emblem/points, that may grant certain rewards within the website they are using. But they do not receive anything that can be transferred out of the ecosystem, in the way of a digital collectible or badge that portrays the communities they follow and engage with. Users retain no real ownership of anything that illustrates the money or time spent engaging with the creators they follow.

Twitch as an application is in essence just a messenger where each user (including the creators) has a profile where they save their media content. The other key feature is video streaming, where fans can chat over live streams, pay subs, and raise their social profiles, within the communities.

We also have a landscape where businesses/organisations host a variety of loyalty schemes on different mobile applications. While digital cards for these schemes can often be stored and used through central apps like Google Wallet, to have a full UX where you can view point totals, etc, you need to have the relevant mobile application downloaded on the device. This has created an ecosystem where devices have become flooded with numerous applications, with multiple logins and accounts. Also, loyalty points that are collected are nontransferable outside of the user redeeming them at the retailers for their reward. Again, users have no real ownership outside of the ecosystem they are engaged with and as an example, they are unable to swap points, with other users.

In short, there is no real standard for current subscriptions or loyalty schemes that we connect with.

A p2p Instant Messenger and toolbox can look to provide the solution to the issues outlined above. As it stands there is not a p2p messenger that has currently managed to capture considerable market share. While the technology to sustain p2p messaging is relatively nascent, it has reached a stage where it is becoming more infallible to be harnessed within a full p2p sphere.

2. The Idea

The idea is to create a fully decentralised IM messenger that will harness p2p technology on a level that is not currently offered by incumbent applications, in relation to the way messages are sent as well as stored. The solution would be underpinned by a private key, allowing p2p messaging, including p2p storage for message archives, user profiles, and media content tied to digital assets.

An early, notable feature to be launched would be video streaming with a chat thread window for creators and their communities. Public or private groups can be created or joined, with direct messages, voice calls & video calls being standard facets for the IM.

To support the IM, the platform would host a toolbox that would allow users to create their profiles and digital content like badges, points, or collectibles. The content itself is represented by a multimedia file, that the user can upload or select from stock content, via the toolbox (to include creation/design in the future). As an example, the content created could be distributed to community members in a chat group, following their levels of engagement. (Emulating the Twitch model, where users receive digital emojis).

This content allows for gamification, where if a certain number is collected, they could evolve into a more premium collectible, granting access to things like exclusive groups or a more enhanced badge, etc. As the ecosystem grows, the digital content could be used to mint skins for gaming (as just one example). Subscribers will be able to exhibit their advocacy for the communities they follow, making subs paid translatable into something outside of just being a digital image within a group.

The other key area to be supported by the toolbox is the hosting of loyalty schemes. The user group represented as businesses and organisations, will create a profile that would link to their loyalty programme, where users could scan a QR code and receive the relevant points to their account on the p2p IM.

There is an opportunity for organisations to reduce costs relating to their mobile applications, due to the infrastructure needed to support their loyalty programmes, engagement campaigns, mobile apps, etc being provided by the platform i.e. their profile replicating their mobile browser or app UI.

The toolbox helps create a standard for user profiles and amplifies the benefits of underpinning certain digital content e.g. loyalty points, badges, and community collectibles, as a standard that would be ultimately NFTs.

What the toolbox provides is a hub for users to create digital content that will have various uses, across multiple industries (both online and offline).

In the long run, the application will be under the control of a DAO, ensuring that along with the technology the organisation itself will be decentralised. What this ensures is that the ecosystem operates with a not-for-profit ethos and is under the control of the users of the platform. Governance like development decisions and proposed protocol fees will be created and voted on by the token holders, allowing for a unique proposition for users to be owners of the app they use and empowered to engage with governance proposals.

The app will be free to use, with user profiles (which will have a measured size cap) being stored on the decentralised storage network Swarm. As the platform grows, storage costs would be paid for by charging a small protocol-based fee, on certain transactions and used to buy the BZZ needed to host user data.

The aim is to build a large user base, where digital marketplace protocols can be bolted on that will disrupt marketplaces like Booking.com, Uber or Bolt, etc. The fees can be charged to further develop the ecosystem as well as cover costs and will be considerably lower than the incumbent intermediary fees. The platform looks to charge a fee in the long run, that would be <1%, which opens the opportunity for a community-voted fee to be levied e.g. 2% on all transactions in a region. This could then be spent on a community voted charitable cause, where the service takes place.

3. Web3 Fundamentals

The app will adopt various web3 fundamentals that will underpin the p2p element of the IM and embrace the principles that have become standard with decentralised technologies. These fundamentals form the technology that will support the ecosystem to grow and help deliver a more enhanced UX.

3.1 Peers - User Groups & Profiles

All users who download the app will create a profile upon registering, which ultimately makes them a peer in the network. The peers can be broken down into 3 distinct groups:

- Standard Users

- Content Creators

- Businesses/Organisations

The notion is that they will each have a profile, represented by a 'sub-ENS', but the content displayed for each would represent different demands with the profile UI/UX and on the amount of data stored. It is important to make this distinction because as an example, content creators and organisations would produce and store more content than a standard user.

Standard users would predominantly store their messages (text files) or multimedia files for their profiles and digital content. Content creators and businesses/organisations would mostly have profiles where they would have a larger digital footprint of multimedia files. For content creators, this would predominantly be their catalogue of streams and for organisations it would be more in the form of different UIs, i.e. a copy of the content from their mobile app or website.

In the long run, the platform seeks to support user groups like organisations to increase their engagement with advocates, by rewarding loyalty with access to private chat groups and exclusive digital media E.g. locker room/backstage content, collectibles, etc.

Profiles will need to be hosted for free, with the cost for storage paid for by a small fee levied on transactions made during chats or streams (see protocol-based fees).

3.2 Private Keys

All users will have a private key. However, this is still an alien thing for the majority of people, but a feature that is being rolled out and pushed by top tech (see article). From this perspective, it’s a great time to roll out a free-to-use, decentralised app, with web3 capabilities, while there is a reduced barrier and rollout (conditioning) when it comes to security (passwords to private keys).

In the short term, the user's private key will be offered as a seed phrase, passkey, or QR code. The QR option will contain a warning about the security of having a key in QR format but will not be heavily pushed due to accounts not having any financial burden. However, if a user starts to store collectibles on their account, then warnings would be sent if the user has opted to store as a QR. (see Account Abstraction*)

What the private key allows is for the user to store digital assets on their account and in conjunction with the toolbox, creates a hub for users to have an interactive messenger not seen before. Ultimately, it allows for digital points, badges, emblems, or collectibles to be simplified into one standard.

3.3 Toolbox – Creating Tokens with Jpegs

While the private key allows the user to store digital assets, the toolbox is the hub that facilitates the creation of them. We've mentioned numerous different digital interactions that we currently have whether collecting points for the various loyalty schemes or receiving a digital emblem or badge for engaging with an online community. All this kind of content can be categorised as the same thing with regards to the front end, being ultimately a jpeg image. The backend code base can become a standard when created via the toolbox, allowing for a more congruent ecosystem and UX.

The toolbox permits users to mint the aforementioned into a universal standard, that is effectively just a token with a jpeg attached. A free-to-use playing field is then set for anybody to join and create engaging campaigns and schemes that can help grow user bases and interactions with advocates.

The toolbox acts as the link between the user and Swarm storage, where the user profile is created and saved to the network, the digital assets created are done so via the user's profile and the toolbox, which basically mints the user's jpeg (which is saved on Swarm) with a token (which is saved on their account).

It's important for us to have a focused approach when launching the app, however, if the toolbox is built correctly, it provides an easy-to-use portal for users to upload or create their media file (image or short video file); and in the long-term release a toolbox that could contain photoshop style features for creation. Any profile can create digital content and set user-defined preferences around the principles of its distribution and uses.

To conclude, we can consider a loyalty point as fundamentally the same as a digital emoji, with the only differences being the image itself and the creator's set preferences based on how the digital is collected/distributed, or used. For example, a loyalty point is something the user collects after a purchase, by scanning a QR code and later redeemed for a reward when a certain number is collected. Whereas a digital emoji maybe something sent on a chat group, from the creator to a subscriber who has earned kudos in the community, which can i.e. grant access to an exclusive group.

3.4 Usernames/Public Addresses. (ENS Sub Domains)

The user profiles will not be linked to a mobile number, but rather a sub-ENS. The user will input an ENS of their choosing and this will act as their username/point of contact. The address would be represented as the following: e.g. NTL.appname.eth/gno*

User-selected ENS IDs as a point of contact, provide a unique opportunity and UX compared with the status quo; mobile numbers or email addresses. A sub-ENS ID is their public address, however, it will not allow open access for other peers to contact unless both parties have requested to connect. (This preference can be changed if the user chooses an open profile). The ENS/public address will also be represented as a QR for peers to scan.

4. p2p Messages

For some users the attraction of encrypted messages not being saved on a server, but to the device only would be the main draw for using a p2p messenger. However, there is also a large user base that would want to save messages, in a similar way to that on WhatsApp with archiving. Naturally, WhatsApp stores data in a centralised manner, but this data could also be stored on Swarm, with encryption, creating a fully decentralised p2p messenger.

The main principles of the p2p messenger will be built on privacy whereby default messages will only be saved locally on the device. However, there will be the option if users want to archive their messages to save on Swarm.

In order to create a funnel for messages to be stored on Swarm we need to harness a protocol that supports p2p messaging. In this, there are a few options available:

4.1 Swarm's PSS

PSS provides a solution to p2p messaging; however, it may not be the best solution in terms of instant messages (IMs) due to latency. The node needs to mine single-owner chunks into specific neighbourhoods (trojan chunks) which will induce latency, creating an issue for IMs being delivered within the timeframes expected by users. For this reason, we will explore other options below that could better serve demands.

4.2 Waku Protocol

Waku is tried and tested in the sense that Status is already utilising its protocol for p2p messaging and companies like Coinbase are currently trialing Waku's protocol for messaging between Coinbase servers, which helps qualify its potential in the long term. This makes it an appealing medium for enabling a fully decentralised IM, once fused with Swarm.

4.3 Status Fork

Taking advantage of the code being open source and that Waku is used, the app could be a fork of the Status app, but a more trimmed-down version relating to the UI/UX. The fork would also need to have the ability to 'talk' to Swarm, concerning messages and account-associated media. The other key difference compared to Status will be the user's ability to select a sub ENS of their choosing, without needing to stake tokens.

Currently, Swarm is not compatible with Status, so any integration needs to be explored.

4.4 Web3 Application Standards

Using a concrete example of building an IM application, applying best practices in write once, use anywhere:

1) Implement core business logic in Rust for cross-domain use between the backend and frontend.

2) Frontend to be written in Flutter to maximise cross-device capabilities

5. Storage and Costs

All data will be stored on a decentralised network and not a central server or IPFS (which still presents centralisation issues). The network used will be Swarm and as the ecosystem builds out the storage costs will be covered by a small fee applied to certain transactions made within the p2p IM. This will provide a free-to-use ecosystem for users, however, data limits would be applied, where users would need to purchase more storage space if their channel is not contributing to the cost of storage.

We look to champion users becoming ‘greener’ with how and what we store digitally and feel strongly that there will be an evitable swing in attitudes, with regards to how much data and what is being saved.

Users need to be able to save data on Swarm securely, where only they will be allowed access. Ultimately, access would be granted to the associated private key, however, this is not currently possible due to the user needing to run their own gateway for exclusive access (see Gateways). Until mobile gateways have been developed on Swarm, users will need to use the platform's gateway to upload data. Alongside this, updates are needed to the network, so the privacy of user data is still upheld, despite the upload being via a third-party gateway (see Pre-Signed Chunks/Sponsored Chunks).

6. App Features & Campaigns

The platform will integrate some key features that will help create a superior UX, as well as enable various campaigns that will all help drive adoption. The various campaigns and features will utilise key functions like messaging and the toolbox itself, enhancing user engagement.

6.1 Video Streaming & Chat Feature

A feature to launch in the early stages will be video streaming with a chat facility. This would allow content creators to stream their content in the same manner as current UIs/UXs (e.g. Twitch) but with a unique UX around the digital content available and user ownership.

A UI where the live stream has a chat window below would need to be developed as well as profiles where creators can archive their streams, all ensuring that the fundamental UX currently on offer is not interrupted.

Etherna provides solid foundations that could be built off for archiving creator content and access to their profiles.

Users will be able to donate to the channel, by utilizing the accounts that underpin their profiles and a small fee will be taken from the transaction.

(EDUCATING USERS ON PRIVATE KEY SAFETY WILL PLAY A HEAVY ROLE IF USERS START LOADING FUNDS TO THEIR ACCOUNTS. ACCOUNT ABSTRACTION WILL BE KEY TO THIS)

6.2 EIP 4337 – Account Abstraction

The app will very much look to pioneer EIP 4337, recognising that storing private keys isn't a user-friendly process. With a core team specialist, we will provide a more enhanced UX when it comes to recovering accounts, following private key loss.

We will be able to implement and spearhead account features like:

- Multi sig/Social recovery - e.g. Friends/family authorising new keys.

- Hardware signers - biometric data like fingerprint or face ID.

- Multifactor Authentication - e.g. email or SMS

The app will look to champion elements like social recovery, where users could select some of their close contacts to be eligible to authorise new keys etc. Also, exploring hardware signers like fingerprint or face ID, to further reduce the issues with private key storage.

Ultimately with an onboard specialist, we will be able to help champion AA, to ensure users losing access to their accounts is a near-impossible event. AA will be key to ensuring that registering and saving keys is as seamless as possible, which will be critical to us driving real adoption.

6.3 Digital Collectibles

In the early stages, digital collectibles will be a key component of user adoption. They provide an opportunity for brands/creators etc to connect and engage with their customers/fans etc, by providing them with something representative of their interest which is interactive/dynamic. The account/wallet also provides the foundations that could form a loyalty scheme where users can collect and cash in/transfer; when they have a certain number or even have the collectibles evolve into a more premium/visually appealing digital asset.

Instead of storing the media content for the collectibles on IPFS (which is a common solution for NFTs today), the content can be stored on the Swarm network. This provides a much more decentralised solution where data is not pinned to a host but stored on a decentralised network.

From a creator/brand/business perspective, the main purpose for users to claim their collectibles is so they have a channel to send messages, leading to further engagement with their community. This could be in the form of direct messages or via public/closed groups. Naturally, the collectible itself is a form of advertisement for the creator and advocate.

The free-to-use toolbox would be provided so creators can design and mint digital collectibles for their communities. ERC 2981 - royalty payments (clip/small fee) would be invoked on future sales of the NFT, when rolled out in the future, which would be earmarked for development and ecosystem costs.

Fundamentally, the digital content created will consist of two components; on the backend is code that is saved to the account in the form of an NFT or FT. The frontend is in essence, media content that will be saved to Swarm and accessed by the account's private key. The media files should be built on existing standards (Jpeg, mp4, etc), to ensure the user does not experience system lock-in with regards to the visual representations of their tokens.

6.4 Decentralised GPT Search Feature

Integrate a decentralised Chat GPT type feature, to be used as a search engine for users.

7. Gamification of The App Ecosystem

The app seeks to grow its user base by creating a platform that encourages usage through the gamification of the interactions that users have with other peers or content on the network. The ecosystem being created would allow the interaction of communities and brand advocates to be in a more enhanced way, allowing for higher levels of engagement and advocacy. We will explore some examples, that have already proved popular when it comes to return rate and enjoyment.

7.1 Decentralised Tinder – Enhanced Graffiti Wall

Providing the features, allowing for access to a free-to-use Tinder could present an opportunity to develop the already established Graffiti wall on Swarm. A geographic consensus layer would need to be created along with some other primitives relating to privacy. But a decentralised dating feature that harnesses already established tech of Graffiti Wall, would provide an enticing option for certain user groups.

Graffiti Wall in itself could prove popular with user groups who are not necessarily concerned with privacy and want to post a public picture/profile.

7.2 Collecting Content – Collectibles/Loyalty Points/Badges

The notion of collecting has long been a pastime and a societal trend that has stayed strong in terms of popularity. In recent times we have seen a growth in users collecting digital versions of Basketball (as an example) cards, where the asset is locked as an NFT. Loyalty programmes are also a staple in our everyday lives, where we collect points that are redeemable for discounts and offers.

The toolbox allows for the creation of loyalty campaigns and their associated points/stamps alongside digital collectibles, in the form of badges or emblems. While loyalty points could be redeemed in the same manner as they are today, customers collecting badges or emblems could see them evolve into a more premium collectible that gives exclusive access to content and is more visually appealing (e.g. gold emblems)

7.3 Gaming Skins – Evolving Digital Content

Gaming presents a huge industry to tap into, from streaming to users playing games themselves. As digital collectibles become more interoperable with computer games, there is an opportunity for the app to be a hub for users to save their content for gaming. Coupled with this, the content collected from communities could be used to form and mint skins and game content, that can be uploaded to interoperable games to be flaunted while playing. The p2pIM account allows the user to store and evolve their digital game assets, for later uploading to the relevant gaming environment. (e.g. special skin or weapon).

Gaming is just one industry that can be revolutionised by evolving content.

7.4 Campaigns for Adoption and Growth

Here is a list of campaigns that are currently in the early stages of conversations, and are just a few examples of the types of markets and industries that would be engaged and supporters of building this type of ecosystem:

Example 1

Partnerships with Premiership football clubs – Football fans who attend football games, traditionally will purchase a programme and maybe a scarf with the teams playing. What the app provides is the ability for the football club to create a profile, and then connect with fans. The connection could start by a user simply adding them or by match day supporters scanning a QR code/NFC, receiving a free digital emblem of the game, thereby opening a connection.

The emblems of the games could be interactive where if a supporter attends and collects a certain number, they could receive a special club badge (e.g. gold or platinum). This could become something that fans strive to collect and are proud to display in digital photo frames or on mobile devices. The interactive element could also be explored where fans vote for their favourite goal or 15-second moment, which could be attached to the emblem of the game.

Each football club would naturally have its own profile, which would have a private area for qualified fans (based on their collectibles held) who are granted exclusive access to behind-the-scenes content.

Example 2

Festivals including Glastonbury are held yearly and attract circa 200k people. Fans attend from around the world and for many, it is an event they attend more than a few times. Currently, there isn't much for fans to collect to document attendance at the festival or any of the performances, other than their tickets or wristbands.

What could be created for attendees, is a digital badge that serves as a memento of their experience. Returning guests could collect and when they have a certain number, exclusive access to a special area of the festival as well as competitions for backstage access could all be explored. These digital mementos could also be broken down for each stage or individual acts, allowing music fans to

document their experience digitally. Favourite moments/songs could also be voted for by fans and attached to the collectible, to make a more dynamic digital.

Glastonbury festival has digitised their ticketing where users need to download their app to retrieve tickets. These could very easily be hosted within the user's wallet/vault, reducing costs for the festival hosting the facility on their mobile app.

Glastonbury is one example of a music festival, that could harness the application to host various campaigns and initiatives e.g. attendees being able to pay at the festival, using their account.

Example 3

Organisations currently spend a lot of capital on hosting their mobile applications and loyalty schemes. The platform provides the ecosystem for organisations to create a profile (that can replicate their mobile application UI) and a loyalty programme by utilising the toolbox.

Users can then collect loyalty points by scanning a medium like a QR code, when making a purchase. The same points could then be redeemed, by scanning a QR code or the user sending the points to the retailer/creator.

Being hosted on a decentralised network will allow users to swap or sell their loyalty points to other peers.

8. The Vision

8.1 Peers & Protocols

Despite the app launching with a heavy focus on NFTs, it is certainly not the main long-term focus of the platform. They will be used and harnessed to grow the user base and aid adoption when it comes to registering an account. The long-term goal is to build a pool of users, who can then be connected by different protocols that disrupt the various online marketplaces.

As the user base grows, it creates a pool of users that can be connected directly p2p via protocols, allowing for txns of a financial nature without intermediary fees. The account allows users to connect with other peers, via protocols that are not geared up toward profit or storing/selling user data (unless users opt-in for data sharing at later stages). Protocol fees charged would be to cover ecosystem/dev costs and will be a fraction of what is currently charged by incumbent markets. (Such as booking.com, uber, etc)

A private key also makes it possible for users to set up things like validator nodes, in a decentralised manner for various blockchains. As the platform grows a key ethos would be that users contribute in some way to the sustainability of the ecosystem. Whether, through protocol fees or by the user hosting their own node, private keys enable peers to help sustain the ecosystems they may interact with and receive a return on their stake. This can take on many forms, depending on the node and devices.

For organisations that have their own mobile applications, there is an opportunity for them to reduce their costs for developing and hosting their app, by replicating their app UI/UX on their user profile. This helps reduce app clutter on user phones and reduce costs for the hosting party.

The main ethos of the platform is to create an ecosystem that seeks to simplify the internet and create a fairer landscape for interactions, which will be simply different peers connecting via protocols.

8.2 DAO

We are creating a DAO, where the ecosystem is owned and governed by the users and token holders. With the DAO operating as a not for profit, the scope is there for an agreed fee that could be levied on transactions, which could be paid towards community voted charitable causes. What would be shareholder profits (based on existing digital marketplaces) could be diverted to more humanitarian and environmental causes in the local area where the transaction was made.

The DAO would ultimately oversee any such campaign and governance decisions around platform/protocol development.

Once the app has launched a manifesto will be released, setting out the pledges and rules of engagement for the newly formed DAO. It will coincide with the expected token sale or incentive based claim (referrals etc), after which decision making will be passed over to the token holders. Proposals would be raised on Snapshot by any token holder and put to the community, where the circulating token supply would vote for their preference.

To ensure the team stays nimble with developments, sub-DAOs will be implemented for time critical decisions.

Control of any community fund would also be managed by the DAO, with proposals for charitable causes being submitted for a vote in the same way that development proposals are submitted.

Nearer the time a full breakdown of the role of the DAO and the community will be mapped out, making its commitments clear and how exactly governance will be managed effectively.

In the short term, daily decisions will be made by the core team and where possible will involve the community in certain governance proposals.

The end game is to create a DAO that oversees and develops a fairer and overall simpler internet, which in essence is a mix of just peers and fair protocols – the end game could also involve laying the physical infrastructure for a new internet network ;-)

8.3 Protocol-Based Fees – Development & Locally Based Charitable Funds

Once the DAO is established the protocol-based fees will be agreed upon by the community. The fee charged that will cover platform costs will be a reducing figure based on the stage of the ecosystem and when fully established would expect an average fee charged for costs to be <1% (hopefully <0.5%). Naturally, the % can be adjusted as per relevant proposals voted, relating to accruing more funds for development.

To give something back to the communities where the service takes place, an agreed cause and % fee could be proposed and voted on by the community. There are a few models that could be implemented regarding how and where the funds are spent, but eventually, when there is a lot of value being transacted through the protocols, the customer of the service could decide which project they would like their fee to be sent to e.g. while on the flight to their destination.

9. Tokenomics

The app would initially launch with no mention of a token. It would not be needed by users to interact with the platform and have no utility within v1.

For users, their first real mention of a 'token' would be concerning the referral scheme where user referrals are rewarded with badges. These badges could be claimed in the future, based on a banding for the user's total number. Also, having options to work similarly to Discord nitro prizes, dependent on partners.

The main purpose of the token will be for governance of the ecosystem, but as the platform grows so will the utility of the token.

9.1 Governance token

The token is an integral part of the platform operating as a DAO. Users will be able to vote on key proposals relating to platform and ecosystem development and operation.

9.2 Staking Native Token - Validator Nodes

Staking tokens for setting up nodes; working in a similar (not the same) way to Rocketpool token. Basically, it can help make setting a node (GNO, Bee, etc) easier - token staked, and the node is created in the back end, based on stake/function. The idea is that the UI/UX is simplified so that a user can set up a node more easily. e.g. staking tokens and saving a few things.

In the same way as Rocketpool, the platform would offer the opportunity for peers to pool funds if they do not have enough to setup a full node.

Unlike Rocketpool, once the node is live, any staked amount of the native token will be a fixed figure for the user (regardless of the token price movement after inception)

In the interim, the infrastructure will only permit users to setup validator nodes via a laptop/PC, which would operate outside of the p2pIM application.

9.3 Staking Native Token - Reduced Platform/Loan Fees

Staking the token could enable a discount on fees and in the long term a discount on loan fees, based on expected revenue (on chain).

Revenue on loan fees could represent a real opportunity to accrue a lot more funds for community voted charitable causes, as well as taking the earning potential for development to a new level.

9.4 Staking Native Token - Share of Fees, Lottery (Benefits)

As legislation catches up to crypto, revenue sharing will be explored, if it can be without upsetting bodies like the SEC.

Numerous other benefits can be explored with the token, also included with staking. Such as extra storage, more features, etc.

9.5 Financing

The token will also be used to raise funds to fully launch and develop the application. Being cautious with funds and token holdings will be at the forefront with the reporting of spend and any centralised concentration of holdings. The main aim is to use financing to create, launch and sustain the ecosystem for a certain period. Then use a token sale to develop further, where after this stage various protocols, with a small, agreed built-in fee, will provide the funding needed to maintain and develop the ecosystem. Ultimately, in the long run, the community pays for itself.

9.6 Incentive/referral campaign

To encourage users to register a private key and sub-ENS, various campaigns will be launched to help support. This would include a referral campaign where users can receive rewards for encouraging others to register. Various other incentives could be built in where the user is rewarded for completing certain tasks e.g. uploading a profile pic or bio.

The incentive will be in the form of the native token, but initially would be displayed as points earned, which once exchanged would be made available for claiming (subject to vesting period).

9.7 Creator Stake

As the p2p environment builds out and becomes more popular, creators will be required to make a small stake of funds, that would act as a deterrent to bad actors. Initially, this stake will be in the form of a fiat value and a set number of tokens in the background that would not see its value fluctuate. Upon launching the token, the number of tokens attested to the fiat amount to stake, will be a dynamic figure based on the market price. If the token price was to drop considerably then the creator would be expected to top up their stake above a certain threshold.

It is important to note that when the stake does become a requirement, the fiat value will be low enough to not deter users but make it expensive for bad actors – circa $20.

Harnessing projects like Kleros, an ecosystem could be created, where bad actors lose their stake, and the reporting party receives the staked amount as a reward/bounty. A code of conduct for the ecosystem will be formulated, spelling out what would be considered malicious and unsuitable for the indexed catalogue that would be hosted on Swarm by the DAO – anything outside of this would relinquish the associated stamp and BZZ that was funded by the DAO.

10. Swarm/Ecosystem Analysis

There are various considerations and primitives that need to be built on Swarm, for a p2p IM to operate effectively. Due to the technology still being very nascent, certain compromises will need to be made about how decentralised the platform can be, during the early phases.

The app will strive to grow with the technology, helping to pioneer the various developments we see as the network becomes more established.

The overall aim is that eventually, all users become Bee node operators via their mobile devices.

10.1 Gateways & Nodes

For content to be uploaded to Swarm it needs to channel through a gateway, which ideally would be hosted by the user. However, due to the nature of the product being a mobile application, mobile gateways need to be developed that would allow users to create their own gateway for uploading content. Until this becomes reality the team would need to host its own gateway so content can be uploaded. While this presents a centralisation issue, it is a necessary step on the road to growing the user base and creating a fully decentralised application organically.

Swarms network is managed and maintained by nodes (called Bee Nodes) that can be setup by anyone in the community, using relatively basic hardware and setup. As the demands on the network grow the number of node operators needs to also, to ensure the low costs and reliability in storing data are not compromised.

The aim is to build up a pool of users that could be easily migrated to, being able to host their own mobile gateways, for uploading their content. When mobile nodes across web3 have become more established, users could be offered the opportunity to create a Bee Node and ultimately incentivised to do so. This could also be implemented as a mandatory feature, where all users would become mobile GNO & Bee Nodes upon registering, thus helping to maintain the network, when they are using it.

Prior to mobile nodes being developed and becoming widely used, other solutions can be explored to help sustain the storage network. These would include plug-and-play NUC devices, that would make setting up a node at home easy, providing the operator a return on their stake and work. The hardware required to setup a node could easily be built into home electrical devices like routers or even TVs. This could allow anybody to have a node running at home, with reduced barriers to setting up and hosting, while still receiving the relevant incentive for doing so.

10.2 Pre-Signed Chunks/Sponsored Chunks

An important primitive that needs to be in place is to do with the principle that currently users cannot retain ownership or have privacy over their data if they upload via a 3rd party gateway, i.e. the platforms. To enable this pre-signed chunks/sponsored chunks need to be implemented, which would allow for user data to be only accessible by their private key, regardless of the gateway used.

10.3 Stamps & BZZ

Users need to be able to delete content if they choose and be confident that any data is deleted from the network. Ideally, stamps would be drained of their BZZ, thus erasing the affixed data, and not wasting BZZ hosting unwanted data or being able to override data within an existing stamp. This becomes imperative when the platform has reached mass adoption due to the amount of DAO-funded BZZ being lost on unwanted content.

11. Digital funds & Onboarding Fiat

With user profiles being underpinned by a private key, it permits the use of digital tokens like stablecoins to be saved to accounts. A payment facility is fundamental to supporting users paying for premium content and will have protocol-based fees levied on, earmarked for the DAO fund.

To help the onboarding of fiat options like Gnosis Pay and Moonpay will be explored.

12. Proposed Roadmap/Plan

The scope mapped out in this whitepaper, could be considered to be fairly broad with regards to the app and the long term aim of the ecosystem. While the overall plan is ambitious, the journey to get there will start with building the foundations/basics, that once established can be developed and built upon.

Establishing a p2p IM that can save to Swarm should form the initial kernel, after which elements like the toolbox should start to be formed and implemented. Once these two primitives are in place, work can begin to grow the user base with the multiple campaigns and features discussed. The idea being we've built an open platform and toolbox, for anybody to join and utilise.

Building protocols that will disrupt the various online marketplaces is very much a long term goal and in the short to medium term, will not be treated as a priority.

Phase 1

Build and launch a p2p IM that can archive messages to Swarm.

- Ensure the user can archive their messages to Swarm, only allowing their private key to access (regardless of the gateway used) – Pre-Signed/Sponsored Chunks
- Ensure that the user can save media files (namely text and image files), that form their profile within the messenger – the portal that enables the user to save on Swarm, will form the foundations of the toolbox.
- Public and private chat groups – the ability for users to create and join public and private chat groups – an archive of the group thread needs to be saved on Swarm.

(Either forking Status or adopting an open-source app)

Phase 2

Develop the toolbox to be an open-source tool for users to create digital content, that stores data on Swarm.

- Users can upload media to Swarm, with the file being underpinned by a token on their account.
- Allow the user to set preferences for the token, to enable the various campaigns discussed to be easily set up and launched e.g. Loyalty programmes or one-off collectibles.

V1 of the toolbox will be more of a whitelist feature available, where campaigns utilising will be used to test and prove the technology.

Phase 3

Build and develop app features that help utilise the toolbox and grow the user base.

- Video streaming is developed and rolled out, ensuring a UI can be delivered, showcasing the stream and a chat window for comments – and ensuring digital content from the toolbox can be sent to the chat groups.
- Allow users (namely creators and organisations) to build a more advanced profile, with multiple pages/tabs and the capacity to store more media content – profiles would be saved to Swarm and assigned to the user's private key for access.

(These features when initially launched, will only be available to whitelisted users)

Phase 4

Aim to roll out the toolbox for all users to access and devise the facility for users to pay for subs and premium content.

- Toolbox open for all users to access (no whitelist)
- Develop the protocols for users to pay for subscriptions and premium content
- Harness fiat onramps like Gnosis pay to facilitate users sending funds.

Phase 5

Develop protocols that will disrupt online marketplaces.

- A focused approach on which markets to develop first, based on user groups on the app.