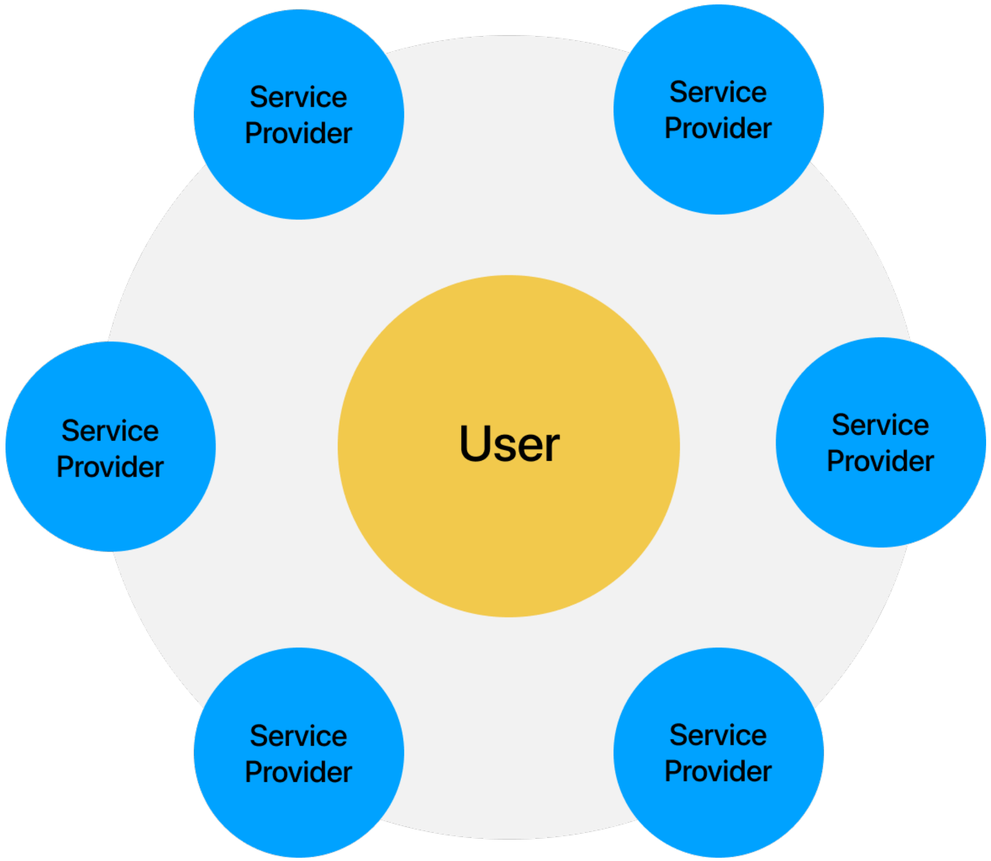

DO WE
REALLY
WANT A
RETURN TO
NORMAL?
ISN'T IT
TIME
WE BUILD

Subnet

Project Overview



Personal Background

- Software builder and serial entrepreneur for 20+ years
- Founded two previous startups in San Francisco and in NYC.
- Co-founded Grouper Networks in 2004. A P2P Social media platform for friends and family. Lead product and tech. <$5M funding. Lead successful growth hacking. Acquired by Sony in 2006 for $65M. Became crackle.com.
- Self-funded and founded a mobile music apps company and got it over $1M USD yearly revenue and achieved profitability in less than 12 months.
- Co-founded Spacemesh, a cryptocurrency based on a proofs of space-time protocol, took it from deck to beta cryptocurrency platform in under $20M with ~20 employees in 4 yrs.

Background

- Social media is harmful. Current platforms are likely to lead to civil wars and even collapse of democracies world-wide.
- Subnet is an opinionated proposal to fix social media by creating a global federated social media platform where users are first and business models do not involved selling of users attentions to advertisers.
- Subnet is designed to provide a viable alternative from current social media platforms.
- Subnet is designed from the outside-in: we started from a desirable user experience perspective and a healthy business model, and designed network protocols and apps to support them.
- We believe that to solve the problem, we must fist replace all network protocols from UDP/TCP and up with modern, privacy preserving stack and next build end-user digital communications apps on top of this new stack.

The World Today - a Ball of Confusion

Contaminated free media

- 57% agree - media we use is contaminated with untrustworthy information.
- 76% worry - false info or fake news being used as a weapon.
- Fake News is here to stay. Used more and more by regimes worldwide to silence critics, journalists and political opponents.

A Broken Corporate Model

- 87% agree - stakeholders, not shareholders are the most important to the long-term success of a company.
- 75% agree - a company can take actions that both increases profits and improves conditions in the community where it operates.

Awareness Rising - Digital Communications Privacy.

- Apps by autocratic companies or monopolies is a big issue.
- 50% of Americans concerned about their personal privacy and prefer not to disclose their sensitive data and decided not to use a product or a service due to privacy concerns.
- The need for better digital comm tools is accelerating with transformation to remote work and social distancing in the age of covid.

Data sources: Pew Research Center & 2020 Edelman Trust Barometer Global Report

Engagement based Corporate Social Media is the Root of all Evil

- Rumors, right-wing populistic rhetoric, and conspiracy theories are always more engaging than the truth which can often be boring.
- Messages appealing to basic human instincts such as **fear of the other**, **the different** and **the unknown** are highly-targeted to psychological profiles of users which are more receptive to such messages - increasing their engagement....
- Fake news spread x2-6 times faster than non-fake news.
- Democracies worldwide are eroding. These platforms are the ultimate weapons for dictatorships.
- They build a reality bubble for each user which is personally tailored to increase engagement. This erodes all shared common-ground and basic shared beliefs which are required to have a democracy.
- We have a moral obligation to provide alternatives to humanity as civilization is in danger by these platforms.

Engagement based Corporate Social Media is the Root of all Evil

I worry because Facebook and Twitter have become giant engines for destroying the two pillars of our democracy — truth and trust.

Yes, these social networks have given voice to the voiceless. That is a good thing and it can really enhance transparency.

But they have also become huge, unedited cesspools of conspiracy theories that are circulated and believed by a shocking — and growing — number of people."

These social networks are destroying our nation's cognitive immunity — its ability to sort truth from falsehood.

- Thomas L. Friedman, NYTimes.

Engagement based Corporate Social Media is the Root of all Evil

Some $1.4trn of the combined $1.9trn market value of Alphabet and Facebook comes from users' data and the firms' mining of it.

- The Economist, `Who owns the web data?`

Fake News - Here to Stay

- Used by regimes worldwide to silence critics, journalists and political opponents.
- Rumors, conspiracy theories and content which appeals to primitive human instincts is by far more engaging than the truth.
- It will keep being a big problem for any communications platform that is optimized for engagement and the problem is inherent to these platforms.

Optimizing for Meaningful Conversations instead for Engagement

- Likes / Retweets / Shares => Quality of conversation around a post
- Followers => Active Conversations. Take the celebrity factor out of online conversations.
- Anonymity can be liberating - content judged based on itself and not on reputation of author. No concern about trolling.
- Different identity for different communities => Better represent opinions.
- Censorship freeness is key.

Moderation, Censorship and Truth

- The role of a digital communications and social media network is not to moderate content - it solely about providing tools for groups to share information between them.
- It is not the role of service providers to moderate information they route between clients.
- The platform is a conduit for any type of information - opinions, fake facts, true facts - it is up to the users to judge what these are, not the platform.
- The network is designed to optimize these goals:
  - Service providers don’t have access to client information.
  - There is no single entity that hosts content.
  - Group creators are super admins of their group and can moderate content in their groups anyway the see fit.
  - People are responsible to moderate information sources based on their

Moderation, Censorship and Truth

Info Middlewares

How to Save Democracy From Technology

Ending Big Tech’s Information Monopoly - foreignaffairs

The New York Times

Opinion

The Coup We Are Not Talking About

We can have democracy, or we can have a surveillance society, but we cannot have both.

By Shoshana Zuboff

Dr. Zuboff, a professor emeritus at Harvard Business School, is the author of “The Age of Surveillance Capitalism.”

Easier said than done...

jack ✓
@jack

Twitter is funding a small independent team of up to five open source architects, engineers, and designers to develop an open and decentralized standard for social media. The goal is for Twitter to ultimately be a client of this standard. 🧵

06:13 · 12/11/19 · Twitter for iPhone

13.9K Retweets **4,890** Quote Tweets

49.9K Likes

Naval @naval · 7h

We're transitioning through a temporary bug in the Internet's history before we knew how to build open social protocols.

At first, the Internet transferred data. Then, it transferred scarcity (Bitcoin). Then, computation (Ethereum). Coming up - identity and social graphs.

258 1.1K 7.8K

The New York Times

Capitol Riot Fallout | Inside the Siege | Visual Timeline | Notable Arrests | Far-Right Symbols

Millions Flock to Telegram and Signal as Fears Grow Over Big Tech

The encrypted messaging services have become the world's hottest apps over the last week, driven by growing anxiety over the power of the biggest tech companies and privacy concerns.

Imagine OnlyFans without the server Inc. overload...

Money and power

Enter Bella Thorne.

A 22-year-old former Disney star with 24 million followers on Instagram, Thorne broke OnlyFans records when she created an account in August last year. After misleading subscribers into purchasing a "nude" photo for $200 (which turned out not to be a nude), Thorne made $1 million in a *single day*, but left a trail of destruction in her wake.

Bella Thorne caused controversy when she launched an OnlyFans account last year. Getty Images

As a result of her actions, OnlyFans was overwhelmed with refund demands. Thorne's representatives didn't respond to a request for comment.

Weeks afterward, OnlyFans limited the amount content creators could charge for "exclusive" content to $50 and changed its payments from weekly to monthly.

Sex workers weren't happy. The payment shift from weekly to monthly was one thing, but for many OnlyFans creators, the ability to charge extra for exclusive content was a major source of income. It functioned as an additional paywall. In addition, OnlyFans put caps on the tips system, which also limited the amount creators could make from their subscriber base. All up, the changes dramatically reduced the amount creators could make from the service.

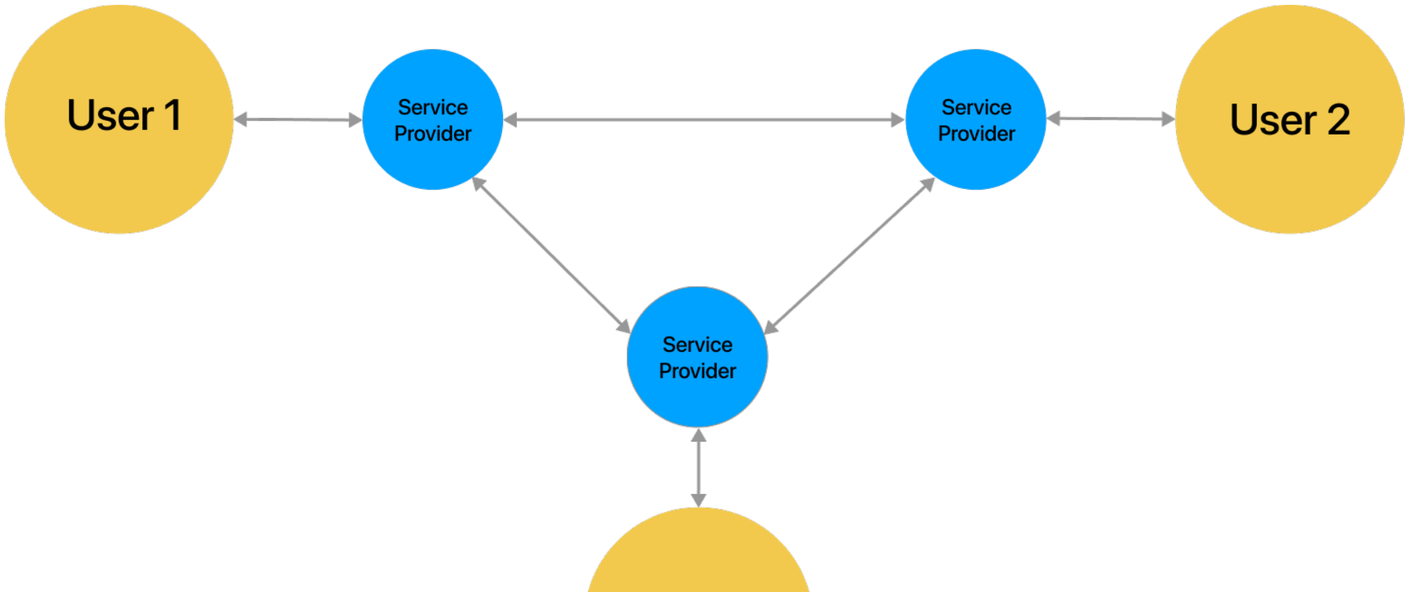
What to do?

- It is becoming widely understood centralized social media platforms are doomed and are very dangerous for humanity
- However, very few propose an alternative...
- Subnet is a concrete proposal for such alternative....
- What's needed is fresh thinking from the low-level network protocols level all the way up to the end-user experience, and an architecture that will work in the real world where people have mobile devices that go offline frequently.

Introducing Subnet

A **highly-opinionated project** designed to facilitate
Inversion of social media and **digital communications**.

- Appeals to some people and service providers, other networks with different design goals and tradeoffs may fit others.
- As always, there is no silver bullet nor one size fits-all…



Subnet Vision

Create **user-centric digital communications apps**
built on top of a **decentralized network infrastructure**

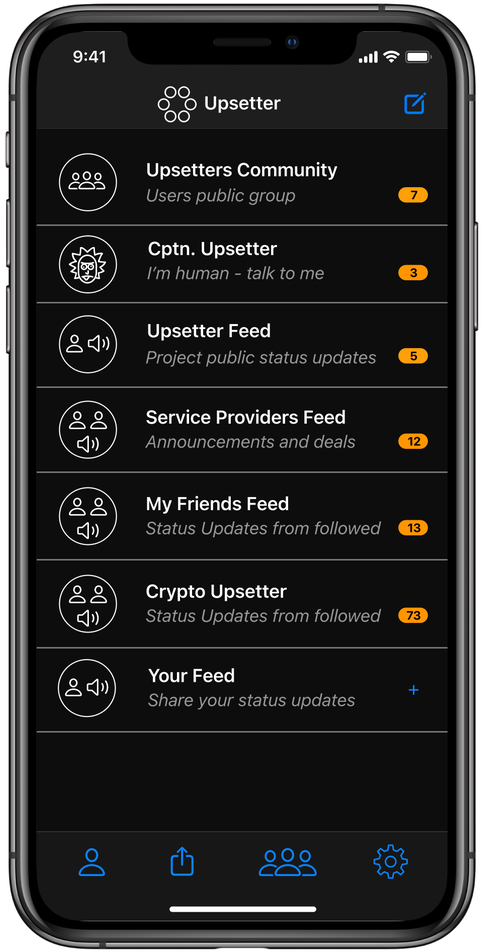
Subnet offers 5 core end-user features:

1. **Instant messaging** - 1:1
2. **Groups** - n:n
3. **Status Updates** - 1:n
4. **Multiple Sources Feed** - n:1
5. **Premium Content** (blog post, image, video, music)

Additional features:

6. **Newsletter -** Premium Status Updates
7. **Premium Groups** - Monthly subscription communities
8. **Limited-Edition Premium Content -** art and fans items
9. **Proofs of Action or Affiliation -** Certification.
10. **Digital Identity** - User-generated based on proofs on proofs of ownership and affiliation
11. **User-to-user** instant payment and all premium purchases.

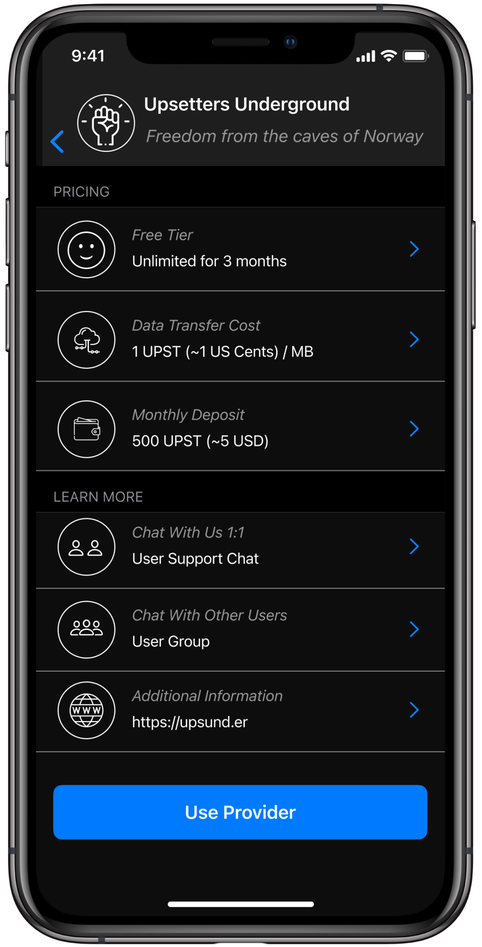
>> Future net services: decentralized storage, proxy Internet servers, video transcoding services, name servers, multi-party real-time video chat, etc...



Business Model

Optimal pricing for ad-free digital communications

- **There's no free lunch**. We all still pay the price of using 'free' services in web 2.0 and mobile native 1.0.
- Service providers have operational costs and need to be profitable.
- We need to design networks which **dynamically and automatically find the optimal price of digital communications** by considering both users and service providers.
- Modern **crypto**, **p2p**, **cryptocurrency** and **blockchain** technologies enable this new model at scale.
- A common network coin is what aligns interests between users, service providers, developers and investors.
- Subnet is such a network.



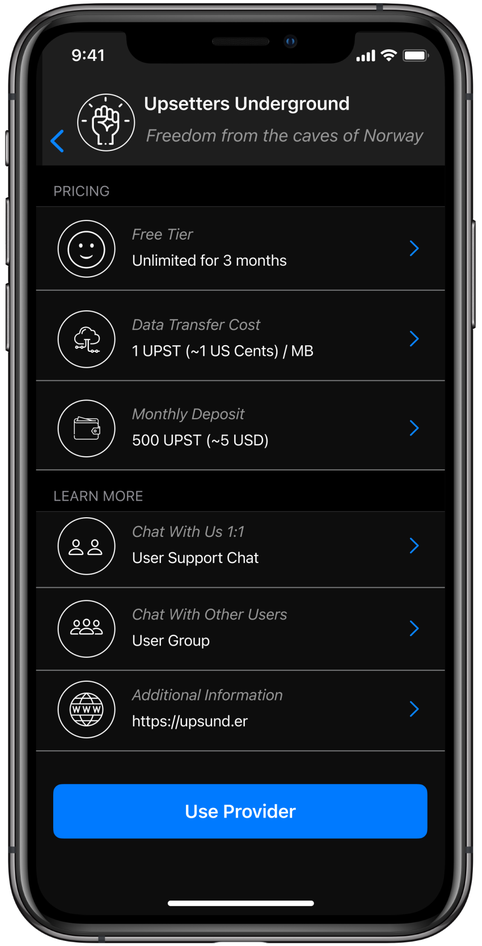
What about Telegram?

1. Servers are closed-source and ran by one company.
2. One company with power to censor users and to provide encryption keys to governments. Censorships did happen.
3. Token to empower user-to-user payment efforts failed due to bad construction.
4. Long terms financing is uncleared currently financed from token ICO proceeds - huge expenses due to need to operate managed servers worldwide.
5. User identity is based on mobile phone numbers - a highly personal identifiable identity.
   Hard to create multiple identities and organization identities. Impossible to be anon.
6. Groups and channels are not end-to-end encrypted and are subject to Governments take-down notices and users doxing.
7. Raised $1B in convertible debt in 2021 - needs to make substantial revenue from ads over next 5 years.

“Previously, when removing posts at Apple’s request, Telegram replaced those posts with a notice that cited the exact rule limiting such content for iOS users.”

“For the last 24 hours Telegram has been under a ban by internet providers in Russia. The reason is our refusal to provide encryption keys to Russian security agencies. For us, this was an easy decision.”

Read this: [five-reasons-you-should-delete-telegram-from-your-phone]

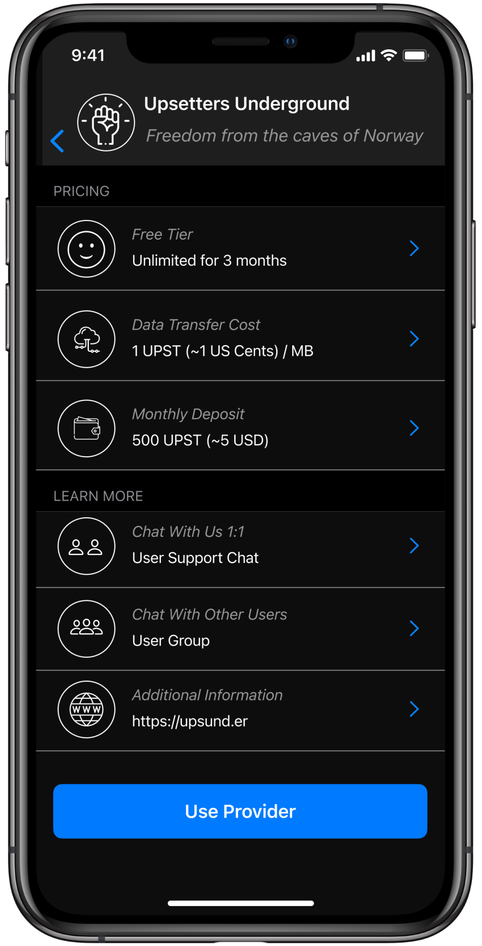


What about Signal?

1. Not clear how it is going to be financed long-term, currently financed by philanthropy of privacy aware parties - huge on-going expenses due to managed servers architecture. $50M contributed since 2018.
2. Users must be identified by a phone number.
3. No payment features - critical for the next-gen of messengers.

“Previously, when removing posts at Apple’s request, Telegram replaced those posts with a notice that cited the exact rule limiting such content for iOS users.”

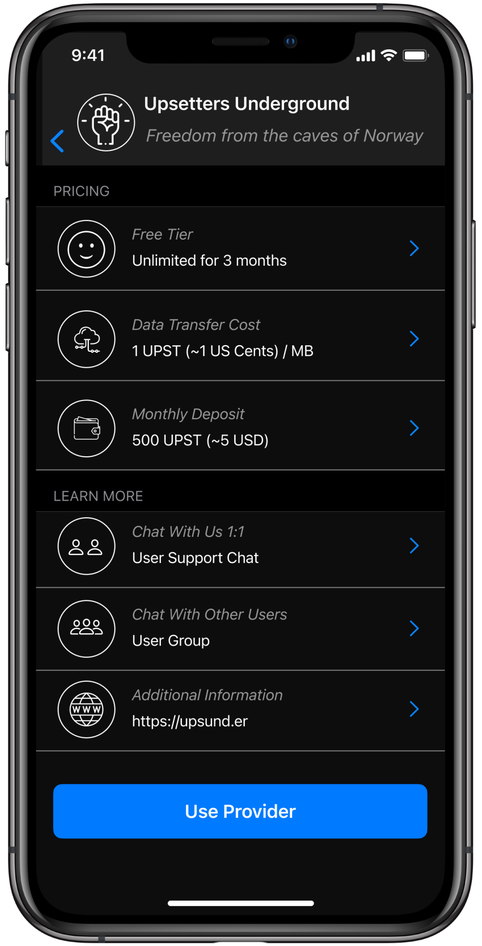
“For the last 24 hours Telegram has been under a ban by internet providers in Russia. The reason is our refusal to provide encryption keys to Russian security agencies. For us, this was an easy decision.”



What about iMeesage?

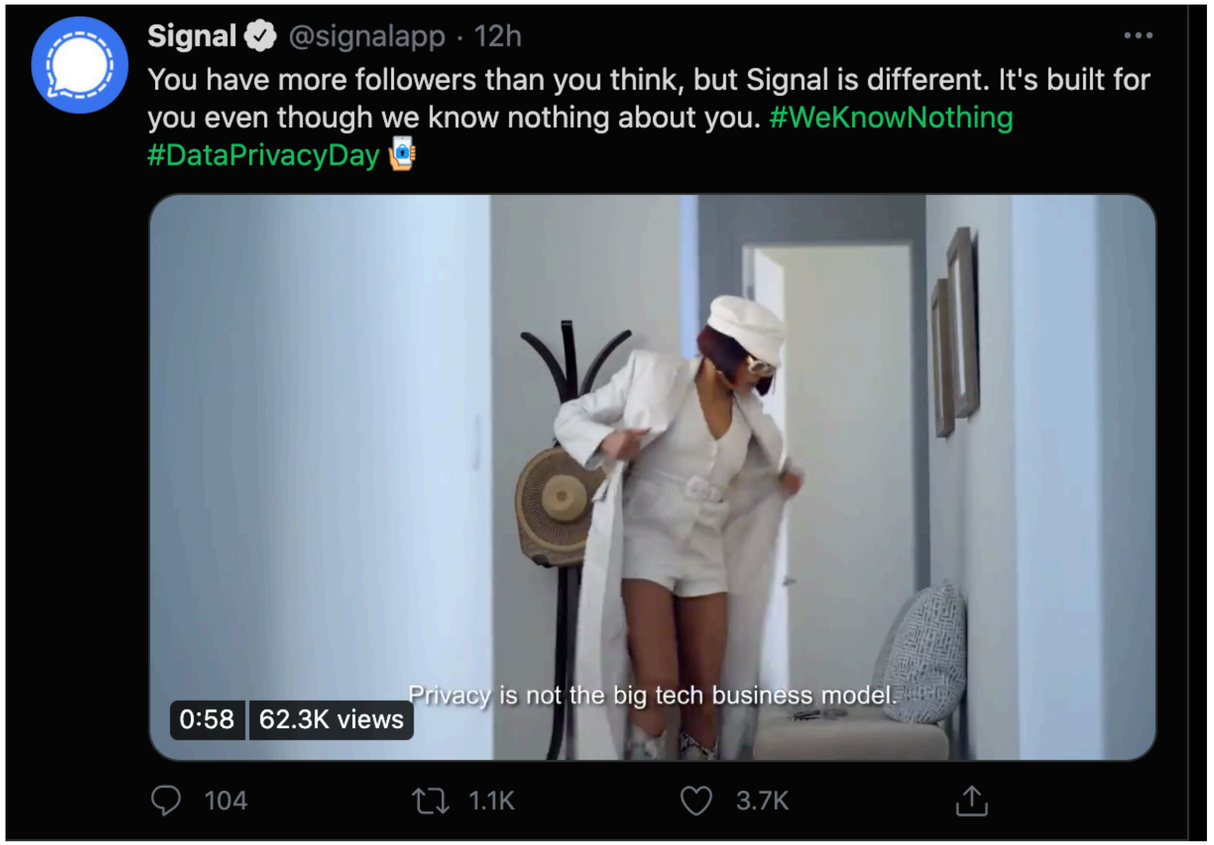
1. As of 2020 iMessage is not end-to-end encrypted.
2. Apple and PRISM have complete access to all user messages without access to your device.
3. Private user keys are encrypted with Apple keys and stored on iCloud servers even when iCloud backup is turned off.
4. UX lags behind cross-platform messaging apps such as Telegram and WhatsApp.

https://sneak.berlin/20201112/your-computer-isnt-yours/



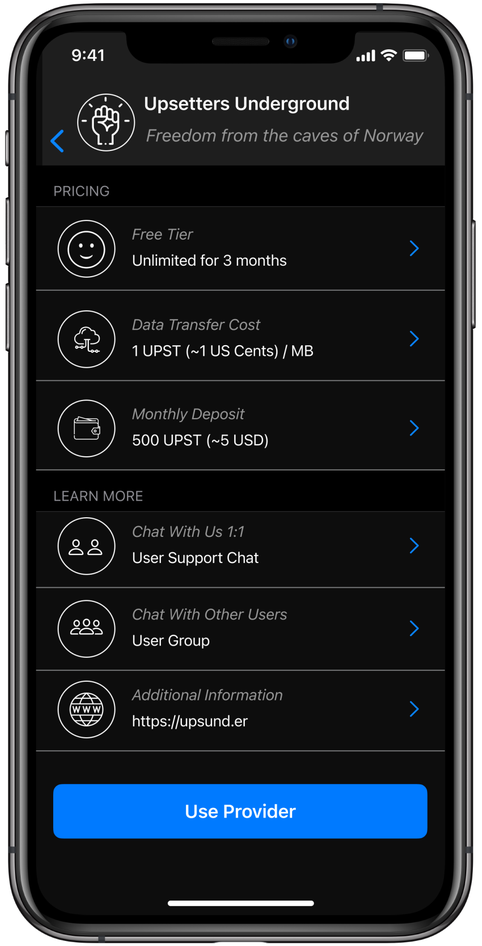
Our solution is to remove the “WE” !

1. Remove the corporation from the platform to eliminate the platform risk.
2. Replace it with thousands of permissionless entities that cooperate via one network protocol to provide the service for users.
3. Simple idea. Next-gen network protocols to make it happen...

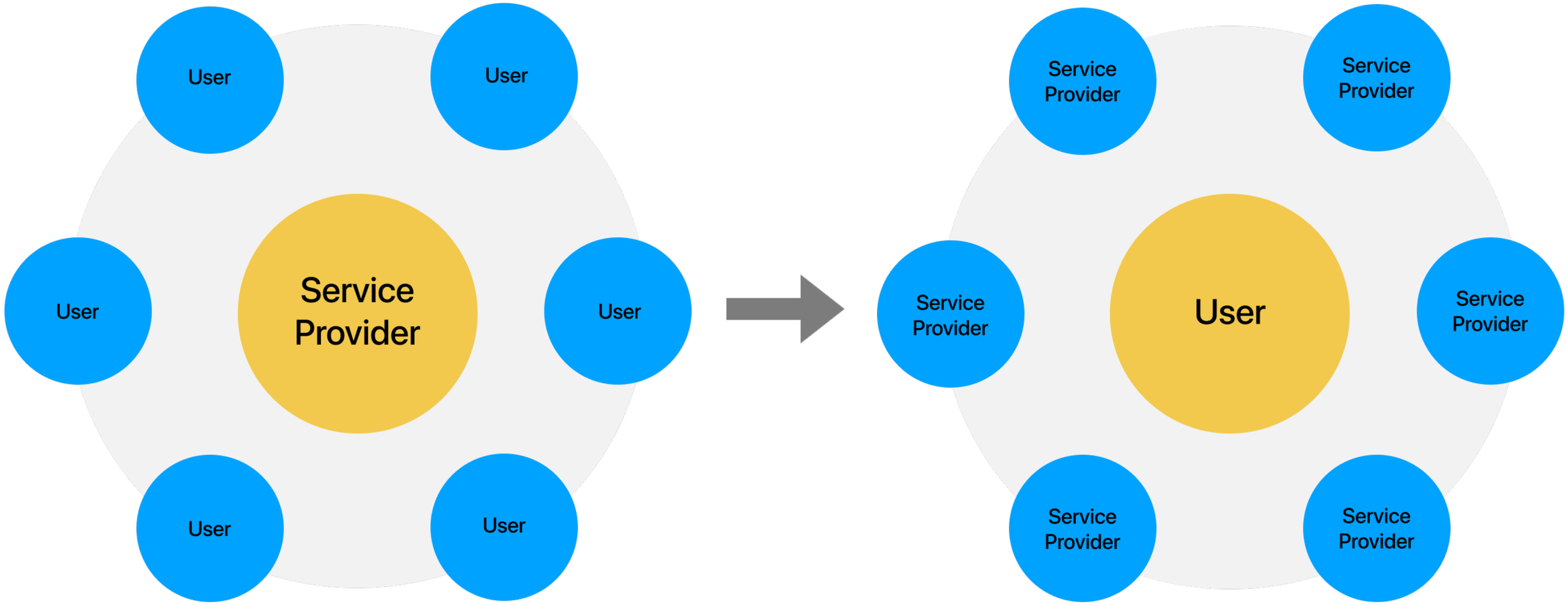


Building an Unstoppable Network for Uncensored Communications

1. There is no company that can censor speech.
2. There is no one cloud infra provider who may shut down the network.
3. There is no company that may be shut down the service or parts of it at any time or change the privacy and terms of service at any time.
4. There are no advertisers interests to reduce the user experience and to encourage engagement.
5. The service works as long as there are at least several entities from anywhere in the world that implement the UNP protocol and provide service for users.
6. By design, even these providers can be replaced at any time if they go down or decide to stop providing service without disrupting platform applications.



Decentralization via Architectural Inversion



Web 2.0 / Mobile Native 1.0

Web 3.0 / Mobile Native 2.0

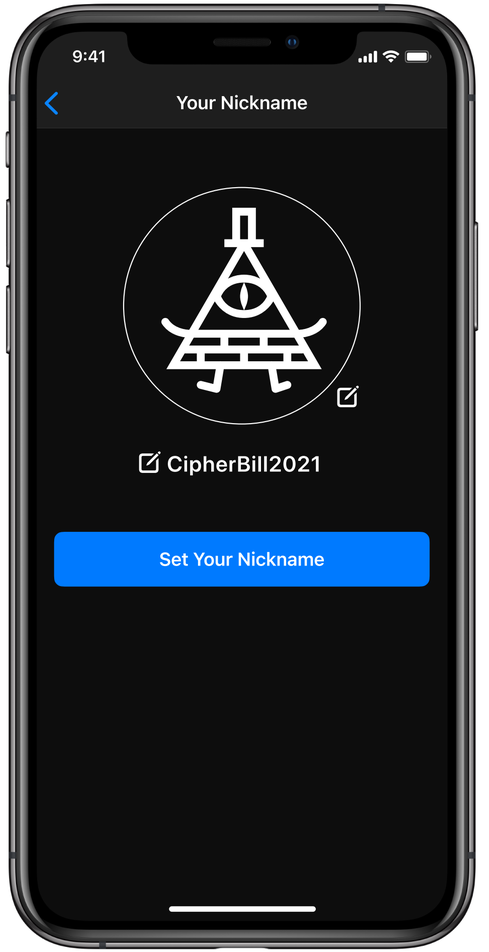
The Digital Dark Ages - 2004-2019

Digital Renaissance 2022?

User-Centric Design

People should fully control their identity. No exceptions.

1. **Personal identification** is at the core of web2.0 due to business model constraints.
2. **Anon by default** - only users decide to be anon or personally identifiable, not the service.
3. Users may use **multiple identities without any limitation**.
   Some may be anon, some personally identifiable.
4. **No content censorship by service providers** - users are responsible to moderate their own created social spaces in any way they may see fit.
5. **No censorship possible on using the network capabilities** by anyone in the world.
6. No clear-text user-generated content stored on service providers servers and providers don’t know what content they are routing between users.
7. **Service providers identity is not personally identifiable** to users unless a provider choses to identify itself.

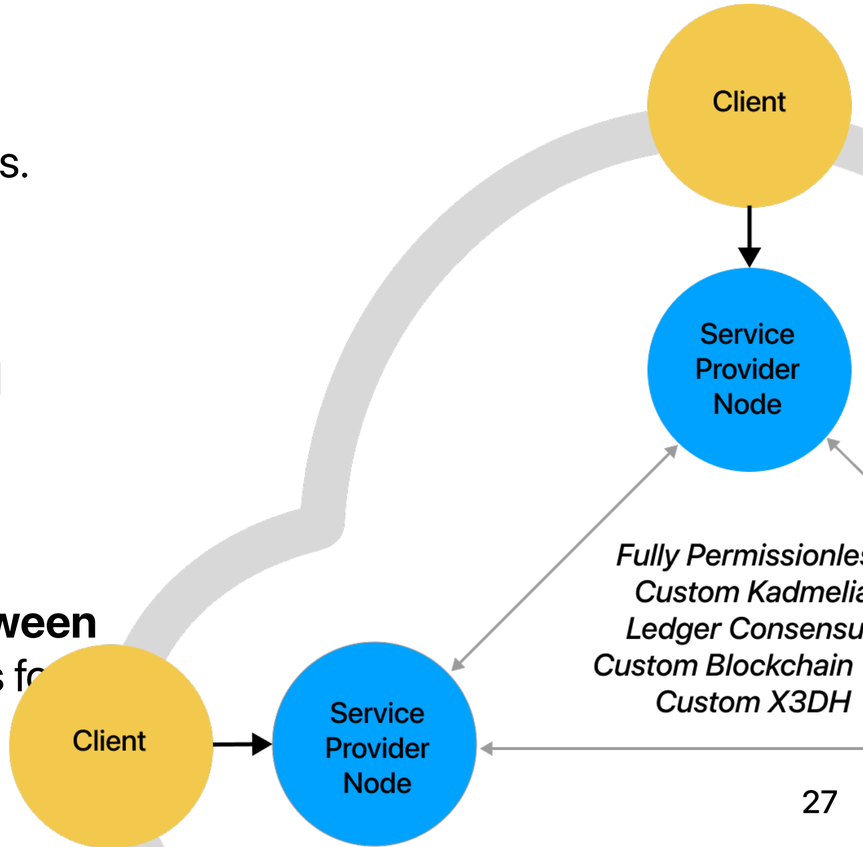


Privacy-first Design

1. Users can be as anonymous or personal identifiable as they want to be.
2. Users always own their data even after sharing it with others.
3. Users fully control who can access shared data. Modern encryption enforce users controls.
4. Service providers can’t access users private data so they can’t use or misuse it in any way.
5. Metadata sharing (a hard problem) is bound to **service agreement**t and to **providers reputation system** and is mitigated by **seamless provider swapping** by users.
6. Rely on **honest majority of service providers** instead of an `honest` monopolistic service provider.

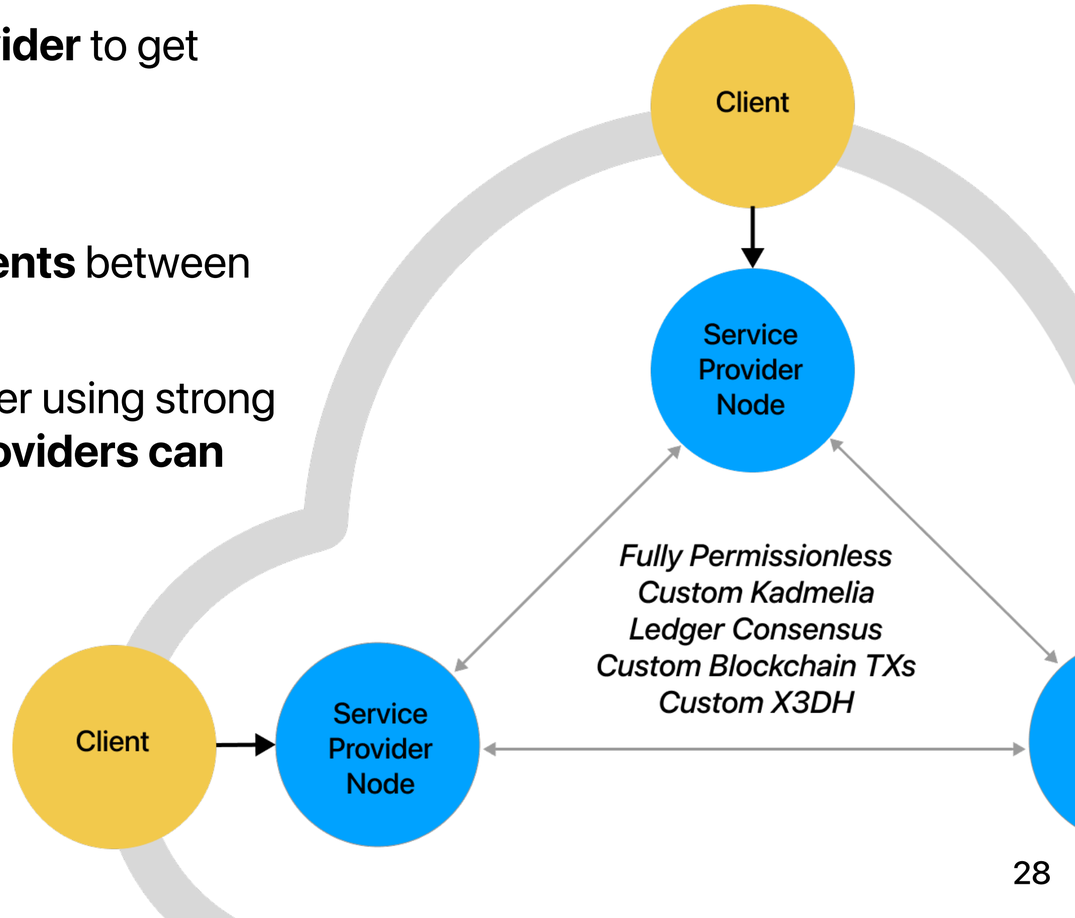
Network Design

- **Users** run **clients** (on native mobile or desktop web) and frequency connect to and disconnect from the network.
- **Service providers** run **permissionless full nodes software** on dedicated servers hardware in data centers 24x7.
- Service providers provide clients with **network services** - e.g. instant messaging, groupware, proxy services and Internet storage capabilities which power user apps.
- Providers form a **custom p2p network** over the Internet and maintain a **cryptocurrency ledger** between their servers.
- Providers communicate with each other using standardized and well documented network protocols such as **decentralized discovery, routing and messaging protocols**
- **Providers never store user's data in clear text. They don't have access to encrypted users data.** Their main role is to **store-and-forward messages between clients on behalf of users**, and not provide long-term network storage or servers fo user's shared data.



Network Design

- **Clients** enable users to create one or more **decentralized identities** which they fully control.
- Clients establish a **contractual relationship** and uses a **service provider** to get network services.
- Clients can **switch to a new different provider** at will at any time.
- Built-in **custom payment channels** capabilities enable **nano-payments** between client and providers.
- **All user data is encrypted** using modern crypto to designated receiver using strong forward and backward secrecy both on wire and on store - **service providers can never read clients data.**



Incentivized Protocols Design

- Nano payments are built into the core protocols. All client to provider messages always include a nano payment.
- Providers are incentivized to provide the platform's APIs, honest results to users, and to lock funds in bi-directional channels with clients.
- Client always uses its provider for network services and does not communicate directly with providers that it doesn't have a relationship with.
- Provider to provider messages - receiver verifies that requester has recently contributed to the network using ***proofs of useful work*** and drops messages from unverified providers.
- Providers must contribute to the network before starting to serve users to establish reputation and quality of service metrics.

Inverted Identities Design

- Public and private parts based on EC crypto - the public key is the public id and the private key proves ownership of the public key by a sentient entity (it can sign).
- Digital signatures to prove attestations - actions, coin holdings, statements, bonds and promises.
- Generalization: **a smart contract based identity** - is configured with crypto key pairs, own cryptocurrency or proves committed resources and has rules about how to modify the pairs and to allocate resources (e.g. DAOs, Smart Wallets). Hardware key used to create a smart identity.
- Cryptocurrency signed slash-able commitments used in network protocols. e.g., payment channels, pricing commitments.
- Reputation is built from provable actions and objective network operational data. e.g. participation in a consensus protocol. Services are delivered to users according to promises.
- May or may not be identifiable to a person or an org - fully at the entity's discretion.

Blockchain & Cryptocurrency

- Blockchain is **just one among several** sets of algorithms, network protocols and data structures running on Subnet to provide its core capabilities. It is going to become a more well understood and mature enabling tech. Think app servers non-sql DBs ~2010…
- Modern PoS or PoST consensus protocols to eliminate security issue with a small PoW networks.
- Optimize for the user - built-in payment channels capabilities with use-case specific optimizations (e.g. long half-open state) , w/o a need for turing-complete smart contracts computations.
- Consensus on a core coin that is paid by users to service providers for providing services.
- A whole range of new kind of subscription services enabled with nano-payments - e.g. seamless news, music and videos…

DESIGN

Instant Crypto Payments

- Automatic and seamless - zero user friction while using apps.
- Cheap - fraction of a US cent. Market-determined prices.
- No transaction fees.
- Key technology for enabling new business model to replace ads.
- Clients hot wallet with spending account funds - low funds security risk.
- Accountable - users should be easily be able to review all payments and to get insights.
- Custom built-in ledger support.
- Optimizations for UX improvements.

User to User Nano Payments

- The holy grail of cryptocurrency as means of payment: scalable, fast, cheap and secure.
- Nobody nailed crypto payments yet.
- Any user is able to pay any other user on the network from any app.
- Enabled by a payment network formed between service providers via incentivized *payment-hubs service providers*.
- A -> SA -> Payment Hub Provider -> SB -> B.

Aren't there alternatives out there?

- **Status.im** - Wrong architecture. Mobile clients are peers in a p2p network. Hard to see how they crack the UX challenges.
- **Telegram** - Identity fundamentally tied to a mobile phone number - a highly personally identifiable id. Telegram Inc knows the personal identity of all members. No sustainable business model. Funded by ICO funds that are in legal limbo.
- **Signal** - no sustainable business model. Funded by good will of billionaires.
- **Matrix** - Wrong architecture. Server per user. Attempt to reuse legacy Internet protocols that were not designed for modern p2p networks. e.g. TLS, DNS, certificates, NGINX, routability assumptions. Not scalable. All content is replicated across all users servers. Expensive to use - At least $20/month for hosted server. There are no decentralized identity servers. $10M+ vc funded. 20M+ users.
- **Freedom box** - Too complex to setup and use. Requires a dedicated home server and home router config.
- Nobody is trying to solve the fundamental problem in a good way considering modern usage patterns. People use mobile clients with limited connectivity and there needs to be incentivized protocols between federation of service providers to build an incentive compatible network.

SUMMARY

Biz Model and Funding

- Subnet is developed and will be launched by Subnet Technologies Ltd - a private development co. The company will hire the dev team and build the platform.
- The Subnet coin is a layer-1 cryptocurrency and not a derived network token with a fixed coin supply. 30% allocated to cover r&d and marketing costs and 70% mined by service providers layer-1 p2p nodes over 10 years.
- The Subnet coin is designed to align all project stakeholders interests and to benefit them. Investors, services providers and builders and early adopters.
- Nano-payments on the platform use a stable coin issued over the core Subnet cryptocurrency.
- Subnet software is 100% open source. The value is in the brand and the network effects of service providers, devs and users around the platform. The co. does not and will own any proprietary IP or any special rights over the network once launched.
- Accredited investors get equity in the company and equity gives right to purchase coin from the co.
- There is current no plan for any public coin sell.
- Think big and build a dev-first team from best Rust systems devs on the plan.

SUMMARY

Subnet - Summary

- Vision to create **user-centric digital communications apps** built on top of a new kind **decentralized network infrastructure**.
- A **highly-opinionated project** that is designed to work in a world where one size doesn't fit all.
- Designed to provide an alternative to **centralized communication apps** and other decentralized emerging platforms that have different core values.
- Focus on **designing the core user-centric incentive-compatible protocols** and on prototyping the protocols.
- Initial **inverted designs for fundamental communication apps** - instant messaging, group messaging and status feeds.
- Aim to build *Subnet* with a remote team of exceptional and passionate creators and builders from around the world - no meta, just building.


DO WE
REALLY
WANT A
RETURN TO
NORMAL?
ISN'T IT
TIME
WE BUILD