Team EFFEKTIO | v1.0.0 | Dec 6th 2022

Introducing: **EFFEKTIO**—an **E**ngaging **F**amiliar **F**oundation for **E**ffective **K**ick-ass **T**eams for **I**mpactful **O**rganizing

An outline for the challenges the team sees for the future of the free internet and goals and motivations behind the project we set out to build.

by Benjamin Kampmann & Daniel Krüger

Table of Contents

Abstract

The free and open internet has been co-opted by large players, and it's all too easy for governments, corporations, and other non-aligned actors to spy on people, in particular on organizers and activists. We, the Effektio team, are building the EFFEKTIO platform to enable privacy-first organizing using strong, resource-aware cryptography in familiar user interfaces.

What We'll Cover in This White Paper

In this paper we share our vision of EFFEKTIO and our outlook on the world out there, in particular in regards to the open internet and free communication.

In the first two sections we dive deep into the EFFEKTIO project explaining what we are up to. The existing technology we are building upon, the gaps in it and need changing and what that will look like in concrete terms.

In the following four sections we share a few observations, trends and challenges we see in a short- and long-term timeframe and the conclusions we are drawing from them.

In the final section we cover the existing landscape of existing tech and will explain where and why they fall short or are not holding up to the challenges we identified in the second part.

Introducing EFFEKTIO

The web needs a decentralized application platform that can hold up to the challenges the world faces. Just think of wars, increased population density and climate change. These are serious problems that we, the people, have to solve. Most underlying technology seems to be available or not far from that, yet, we are missing a starting point to get that into people's hands. In particular, we see a significant lack of available apps with a focus on the average Joe (rather than corporate employees). That's why we are proposing and are developing EFFEKTIO.

EFFEKTIO is a mobile-first matrix-backed Web5 end-user application for casual organizing of social groups.

Casual, social Organizing

Under "casual organizing" we summarize all organizing activity outside of paid work - essentially all groups that would work best if they had a project manager, but simply won't pay anyone to do that, nor have anyone willing to take that on voluntarily. That can be the sports or hobby club, the family's grocery list, the union or neighborhood assembly, the activist group or meetup or volunteer foundation or NGO - anything that is primarily peer-to-peer-driven and runs best on high transparency, social trust and cooperation.

Human-centric social design

EFFEKTIO combines two innovative, new ideas into one app: casual organizing apps and privacy-first data types, yet its most important area is the user-centric User-Interface and Product development. As these apps can't be 'mandated' from the top by an employer or have dedicated people taking care of them for the team, they need to be intuitive, quick and easy. They need to become as casual and easy to use as WhatsApp messages are for anyone from 10 to 99 years old today.

Matrix Structures and Apps

The app itself uses the Matrix protocol for message passing and its "spaces" rooms with a specific "subspace" definition to segregate it from the common chat-room. Effektio extends the protocol with a state-machine and messages around them to provide the social and casual management tools these groups need.

These tools range from a dedicated announcement format with comment sections and likes, over "stories" (in the social setting), Todo-lists with tasks for simple project management, co-budgeting[1], vaults for sharing secrets and passwords, a social forum for more structured discussion, video and image sharing, polls and voting[2], event management and meeting coordination and more - openly and transparently specified and implemented for everyone to copy or build an implementation themselves.

In the spirit of fully leveraging Matrix, each "state change" of that state machine is encoded as a matrix-event in the room timeline - giving full transparency over the entire change history, yet providing a good scaling solution by separating in rooms.

Privacy by default

Thanks to Matrix and its (meg)Olm[3] implementation all room data, including messages, is end-to-end-encrypted by default. EFFEKTIO is the first application platform where all data is modeled from the ground up to have all state transitions or attachments exchanged end-to-end-encrypted and opaque to the servers relaying and hosting them. For further protection, especially around some metadata that is required for proper routing, data for a room is only shared with the servers with users actively participating in the room.

This inherently means that while the final model is constructed from these end-to-end-encrypted messages, there is no single database available aggregating the state for the client ahead of time. This model fundamentally changes the way

---

[1] https://guide.cobudget.com/article/4-getting-started
[2] Loomio Inspired: https://help.loomio.com/en/user_manual/getting_started/
[3] Megolm is the Group-Encryption protocol (also used by the Signal Messenger). Details at https://gitlab.matrix.org/matrix-org/olm/blob/master/docs/megolm.md

developers have to think about their data types and interactions with them to make them work. We call these “privacy-first data types”.

Permissions where necessary

In EFFEKTIO, all apps and activities are inherently social. While users could still open an account and just use it for themselves, the entire concept revolves around rooms to share and access them together. Although our primary target is groups that have some established social bounds and thus some degree of social conduct, Matrix has built-in support for various permissions - allowing us to limit access to sending certain messages to key people or people above a certain “power level”.

EFFEKTIO extends upon this and has an object-based permission model installed in its state machine mechanism, allowing for fine-grained control of which interactions are allowed for each user or a group of users for a particular object.

User-driven Apps through WebAssembly extensions

One specific technical extension EFFEKTIO is developing for Matrix is allowing room members to upload WebAssembly (Wasm) blobs into the state of their room, which can interact with the room or enable the client to interpret events in a custom manner for the room. These can be checked and verified by any other client by executing them-similar to how smart contracts work. A simple example would be a custom automation in a room to create an announcement when the last item in a to-do list is checked off - auto generated by the blob and certified as valid by all other clients, despite the original user not even having the permissions to send news usually.

Through this mechanism we expect to allow for innovation and experimentation from a much larger audience and at much faster pace than the spec process would allow for. Furthermore, extensions that become widely popular and hardened through usage can then still be specified if useful or necessary.

Sharing is caring

But social and cooperation in EFFEKTIO is not limited to people within the group. Groups can also share “app templates” with each other or the public, allowing for massive knowledge transfer and reduction of tedious work. The Wasm extensions just mentioned right before are an obvious yet not very tangible example, but think of todo-lists shared by activist groups on how to organize a protest or a template for meeting notes or news for invites.

Federation first, p2p soon after

As already mentioned above, Matrix is primarily a federation network right now. That already allows it to be deployed behind country-blocked firewalls today, but not yet in totally offline or DNS-less scenarios. That, however, is an area of active development of the Matrix Foundation. EFFEKTIO, too, has a keen interest in getting that ready and well integrated into the app- including features to organize ad hoc-, mesh-wifi-, and bluetooth-networks for short-range data transfer.

Building peer-to-peer support, however, has lower priority than building out the proper infrastructure, state-machine and apps for the end users, all of which can already be used in the federated environment. The lack of peer-to-peer support should not be blocking development or launch.

Federation is a big chance for adoption: For most goal-driven value-oriented organizations, sovereignty over their communication infrastructure is very important. That, unfortunately, means that these organizations, NGOs but also government agencies and citizens lock each other out through mere usage of their tools. By building on a federated network, EFFEKTIO allows every organization to run their own system, if they so choose, yet communicate and organize with any other organizations without switching out of their usual app.

The development challenge

We have to ensure that our team is iterating fast on these. As most of the apps are new in their nature and the underlying data types are yet to be fully developed and understood in practice, the specifications are only made official when it is clear

that it won't change in a backwards incompatible manner. However, as all development happens in the public eye and they are all modeled after state-machines with distinct behaviors, following latest developments should be feasible to follow.

Development, Rollout and Distribution

EFFEKTIO has the aspiration to change the world and offer a significant contribution for people to stay connected and organize effectively throughout the challenges we see ahead. But as with any other project, it starts with a seed and that seed needs to be nourished for a while before it can grow and blossom. That's why we chose to establish a company to build the first iteration.

The code is publicly available under an Eventually-Open-Source-License. This is a temporary measure to protect others from just stealing the code without contributing back. While the larger, long-term governance mechanism needs to be developed later, this company is driving development, rollout and distribution until then. Despite all that, all specifications will always be open and free from patents or copyrights that would restrict anyone else to build an alternative client implementing these standards.

To pay for initial and continuous development, the current revenue model sees two major sources of income: Freemium subscriptions and partnerships with NGOs for good causes.

Freemium Subscription

The current idea to fund development long-term is through getting actual users to pay for it. For once because whoever gives the money also has the most say, and in our opinion it should be the users, not some investors, big corporations (through advertising) or governments (through grants), it should be the actual users. That ensures that whatever is being done is first and foremost in their interest.

However, it is unlikely that every user will be able to pay for the app. That would also restrict its potential adoption, especially in poorer countries. Hence, the current thinking is to allow anyone to use and join the app, set up their family or friends group. And only if you need special features that interact with the wider

outside world, like integration with third-party services like Instagram or a chat on your website, would the user have to upgrade the account to a monthly premium subscription.

Thus allowing for wide, free adoption, yet generating revenue from pro users.

Partnerships with NGOs

The other major path to drive adoption and distribution is through partnerships with NGOs. The EFFEKTIO company won't be able to run servers in every country in the world or host every person or smaller activism group. Instead we want to cooperate with established for-good NGOs, in particular the ones fighting for human rights, climate change, freedom of press and alike, to enable them to run servers with the company as a support backend, and distribute the app among their volunteers and people they support. A branded version of the App would be an obvious extra they'd be paying for, aside from support, consultancy and extras they'd like to have developed.

EFFEKTIO

Engaging

The EFFEKTIO platform and app needs to be engaging, which is achieved from its social nature and modern usability.

Familiar

Despite fundamental shifts in apps available in EFFEKTIO, the look and feel is not that much different from other modern social apps -it should feel familiar to the common user, both in design and look and feel but also through connecting with familiar faces from the actual social circle they know.

Foundation

While initially built as an end-user facing App, EFFEKTIO understands itself as a Web5 development platform for many “casual organizing” apps and a variety of adoption areas.

for **E**ffective

The previous generation of social media has focussed on the “media” part of the equation, promoting (pointless) user generated “content, content, content” over everything else. EFFEKTIO is different in that its focus is on actually being effective: effective as an App; effective for the user; and effective in that the users achieve their goals. Even if that means cutting through the noise, focusing on less and higher quality content with actual value.

Kick-ass

We believe in the power of the people, of bottom-up organizing and cooperation over competition. The goal of this platform is not to promote harmful ideologies or disinformation under the disguise of some weird understanding of free speech but correction and moderation through the social circle. We believe that within that

lies the power for drastic social change that benefits everyone. The people we are building EFFEKTIO for are those kick-ass leaders and members of these social movements, with a focus to be stellar with one another.

Teams

While technically “groups” is probably the more appropriate and technical neutral term to describe the foundational social entity in EFFEKTIO, the core focus is on peers close to one another working towards a common project or goal - whether that be organizing their sports club, coordinating the care work that is a family household or investing time bringing together the local neighborhood or workforce. Teams is the more fitting term to describe that.

for **I**mpactful

Through interweaving social groups and their work tools in a casual yet engaging and fun mobile-first setting, we believe we will enable people to make larger impacts than they have been able to do otherwise. Technology always needs to look at the impact it has, good and bad, and recon if it needs to change its ways for the greater good.

Organizing

“Casual organizing” is the core activity within EFFEKTIO it is only fitting to put that word within the core claim. Organizing as in project management, people management but also coordination and cooperation between peers and social circles is front and center of all apps in EFFEKTIO.

The world is changing, it is changing ever faster and for the worst

The global village is no more

In the jolly ol' days when the internet was young, the idea of the 'global village' came about: the entirety of human kind connection in one global network, where everyone could freely communicate with anyone else, where there would be no borders or walls and it would connect us all together and facilitate understanding of one another.

It's hard to pinpoint when this idea died: was it with the Patriot Act of 2001? When the first and second generation of internet companies started dividing it up into neat little silos under their control? Or when Snowden revealed that the NSA had spied on everyone for a decade? When China put up the great firewall or when Saudi Arabia gained access to all Blackberry devices? When the European Union tried to block websites they disliked or when the FTC decided that not all data is equal or when the governments turned off the internet in Syria and Egypt in 2011 to stifle protests for the first time[4]?

The reality is that the idea of the global village is dead. The internet in Western Europe is vastly different from the internet for someone in China, in South-America or in India. Not only because there are governments trying to block or slow down access, but also because access is not distributed equally in the first place. For many people in the global south, a data plan for their smart phone is too expensive, but WhatsApp and Facebook are included- to them Facebook *is* the internet. Other parts of the world simply have so little bandwidth or coverage or outages that it is more efficient to fly data in over planes from the neighbor and distribute it via usb sticks[5].

The truth of the matter is, no matter how cheap many of us in the "developed countries" think Skynet or blips over the desert might be in comparison, it is just

---

[4] https://news.yahoo.com/news/syria-shuts-down-internet-contain-revolt-212117279.html
[5] https://www.youtube.com/watch?v=fTTno8D-b2E

not economically feasible to cover all last-miles for any profit-oriented company. While the ideal of a globally connected world with high speed internet access everywhere is still something we should strive for, it doesn't seem like we will reach that state (or anything close to it) any time soon.

Borders, fences and walls

While a lack of global infrastructure is mainly the result of economic decisions by large corporations, enough political will could in principle bring planet-wide coverage. However, we are seeing the opposite emerge more and more often: governments from all over the world, mostly authoritarian but also from democratic countries, restricting access to the internet for their citizens or the freedom within it, temporarily or permanently. All over the world we see an increase of governments overreaching and blocking, censorship or outright turning off the internet[6].

Currently in the news are the cut-offs in Iran, but let's not forget that the US Patriot Act of 2001[7] paved the way for the massive internet surveillance apparatus that Snowden later revealed to the world. In the name of security and stability, many governments, including in many democracies, are discussing restricting access or infringing upon the privacy of their citizens or, like China, just replacing the vast majority of services with their own controlled variant instead.

Blocking is not the only form of government control. As Snowden revealed in 2013, it is actually the intelligence operations of the so-called "free world" that spy on everyone's messages and track every move. Although that has seen a loud outcry in the media and civil society, democratic governments have not stopped trying to get even more of these measures passed under the disguise of some unproven "need for security". Even though it was struck down by courts already in the last few attempts, even the so-described libre-left German government has a law proposal in planning again.

---

[6] https://www.accessnow.org/internet-shutdowns-2021/
[7] https://en.wikipedia.org/wiki/Patriot_Act

Yet we need more communication

Climate change is a challenge to humanity like no other before it. It will require more coordination and communication on every level, while the effects of it will make it harder and harder to keep a solid infrastructure for it up and functioning. And yet, to keep our civil societies in-tact, we need more communication, not less: To prevent wars we need to talk to one another. To understand what challenges lie ahead, we need to share scientific data. And as mundane as it sounds: to get that wind park accepted and built, you need to talk to the neighbors. Bottom up, local-first community-oriented communication will be critical for human kind to survive this next century.

While we are facing a degrading communication infrastructure all around us and less global access overall, we have to rely on trust-worthy, uncensored communication more than ever before to sustain ourselves and our communities. Communication across borders and communities is not a nice-to-have, it's crucial for any kind of progress. We will not make it without it.

Conclusion

All technology that works under the assumption of having continued access to a constant global internet is doomed to stay a privilege of the rich and powerful. Any technology that wants to bring about radical change for the masses needs to work reliably in the local-first non-global-accessible-internet setting of a regular smartphone.

Social Media is dead - being social is not

Retracting from the public square to the private circle

A global trend we have seen going for quite a while is that the line between what we previously called "messenger" (e.g. WhatsApp or Telegram) and "social media platform" (Facebook, Twitter), has become very blurry: Telegram Channels allow to communicate to a large audience, WhatsApp Status Updates and Signal's Stories

are uncanny copies of the same Instagram feature—yet with one crucial difference: they are shared in a much smaller group of people.

Overall we can see the pendulum swing back in the opposite direction from everything-is-public: groups getting closer, smaller, more intimate and peer-to-peer — if through shared content like on tiktok, where anyone can become the star in the niche (not only the ones with the massive following), or the WhatsApp family group that is encrypted by default.

While Jack Dorsey's Blue Sky or Facebook's Meta Metaverse try to build a new everything-visible-for-everyone public square, the usage trend is clearly going in the opposite direction. And why shouldn't it? After all humans are social animals that live in more or less static social circles. These smaller groups offer more social control, addressing problems like moderation and combating abuse in a more confidential and human-oriented fashion.

Advertisement killed the Social Media Star

Not only because of that, but also as a side effect of it, the big advertisment-driven social media giants are dying. While it might just be okay to show an ad between a public stream of videos on TikTok, on youtube or between two instagram stories, it surely feels like a breach if that popped up in your friend WhatsApp group or during a Video call on Signal. Not the least because them being encrypted implies a certain degree of privacy, it would simply be considered a rude interruption to get in between an actual "social" interaction.

Telegram and Signal draw from wealthy donors with big pockets (though the latter has diversified their donations in recent years). While it sounds unlikely that Facebook ever will, Musk is trying a subscription model for Twitter after his takeover (which failed miserably in its first attempt), so does Youtube, LinkedIn and Medium—all have a freemium-model, as a significant if not the main source of revenue for the future. They all offer, as part of the perks of going onto their subscription, a reduction in ads shown[8].

[8] Which is odd in and of itself from an advertisers perspective: as this means the most wealthy and solvent of users are excluded from seeing the ads.

Which does make a lot of sense, since the "if you are not paying, you are the product"-model has widely become accepted as the way things are done, and everything on that platforms is public for a reason: so that the prying eyes of both "the algorithm" and advertisers can milk it for data, aka "insights". The upsetting stories of "I talked about XYZ with my friend the other day and ever since I saw ads for it" are commonplace right now and though probably not even true[9], they show how the awareness has shifted and how upsetting this idea is to people.

Global Platforms are easy to shut out

During the Arab spring in the early 2010th public social media platforms like Twitter and Facebook played a significant role in organizing the uprising and protests[10]. Not only the world stage noticed, but also repressive regimes. As a result we see autocratic governments more and more often limiting access to these platforms during protests like in Iran, Hong-Kong, Yemen, Saudi Arabia, Kashmir, etc or even ever ongoing like in China or North Korea. Shutting them off is fairly easy, as these social media platforms need access to known central servers to operate.

Some projects, most notably Signal[11], offer some proxying solutions to allow for traffic to flow through other servers, which are still reachable[12]. However if the governments feel utterly threatened, they just shut off access to the outside world or to the internet entirely in certain geographical areas—rendering anything that requires access to the global network useless for the user[13].

---

[9] https://techcrunch.com/2018/04/10/zuckerberg-tells-congress-facebook-is-not-listening-to-you-through-your-phone/

[10] https://www.researchgate.net/publication/234040341_The_Role_of_Modern_Technology_in_Arab_Spring

[11] https://signal.org/blog/run-a-proxy/

[12] Leading to a fun whack-a-mole situation with local authorities

[13] This also applies to almost all blockchain networks, which, too, require access to the global consensus network in order to function.

Conclusion

What we call “social media” today is going to change drastically. While platforms with a massive following will continue to exist and entertain the masses — the public squares, where the majority will consume and a minority produces — but what people consider their ‘social app’ will be much more local-first and community focussed, intimate, smaller and peer-to-peer oriented. The artificial distinction between that and a messenger will be a thing of the past. A lot more group coordination, ranging from the mundane up to organizing global protests, will run in these spider-web encrypted networks, rather than being publicly broadcasted.

Web3 over-promised and under-delivered

Blockchains require too much infrastructure

A lot has been said and written about the vast amount of energy the biggest blockchains (Bitcoin and Ethereum) require and the pollution they cause (to the point that coal power plants that would otherwise be taken off the grid keep running just for bitcoin miners, who bought them[14]). And though big steps have been made here, most recently with Ethereum 2.0, they tend to overlook that as an actual end-user product Blockchains require too much infrastructure and are way too expensive to run.

Not only for the massive requirement in bandwidth and storage on disk, but most importantly in the core of their architecture: they are intended as a global ledger and as such require a continued and stable connection to the global consensus network[15]. As we've shown above, we consider this a vital design flaw in the overall design of any global blockchain network, rendering it useless for large parts of the world for the foreseeable future.

Blockchains are too costly

Even if you consider having a stable connection an acceptable requirement for running your app or service—and we know all cloud-provided apps as of today do—the vast amount of data that a blockchain typically requires to run far outweighs their value. The Eth2 full-sync is at over a Terabyte as of the time of this writing[16]. Each full-node out there has to have this storage. While it is not practically necessary to have ten redundant copies distributed all over the world to sustain even the largest possible disasters, we keep copies of rather useless

---

[14] https://www.theguardian.com/technology/2022/feb/18/bitcoin-miners-revive-fossil-fuel-plant-co2-emissions-soared

[15] Even sharding and other scaling solutions do not work on your computer while you are disconnected from global consensus. In fact you can be sure that whatever transaction you do locally, they won't succeed once your connection recovers.

[16] Ethereum Full Node Sync "1050.02 GB for Nov 29 2022" according to Etherscan.io: https://etherscan.io/chartsync/chaindefault

information in thousands and thousands of editions. That is an overall cost of the network, which is eventually expressed through the price a transaction costs.

Though the bet that Moore's law applies to storage as well has mostly been true so far, the growth in copies has outran the decrease in storage costs. Even if you assume that cost can actually be brought down to sustainable levels, storing thousand copies on Ethereum will always be costlier than having the data only on one or two federated servers. Especially for less valuable data like text messages between friends, the cost associated with blockchains will remain too high. Technology has always won because it was the cheaper alternative, but for almost all "legacy" web2 technology blockchains are the more expensive, less efficient, less ergonomic alternative.

Conclusion

Blockchains, and with it Web3, have been hyped and over-promised but ended up under-delivering. While there is certainly some use case for blockchains as part of token-exchange mechanisms for the world, it is way too expensive to use for — necessarily cheaper — everyday activities.

Web2 + Web3 = Web5

There is no turning back

As much as you might love or hate blockchains, no one can deny that they have changed the world and the technology landscape. For once encryption (or 'crypto') lingua has made it into the mainstream and overall understanding for the underpinnings have exploded. Research in 'crypto' has seen more money than ever before, big leaps have been made and many aspects about decentralized and peer-to-peer networking tackled or simply solved. It has never been so easy to "deploy" your own custom decentralized network as it is today.

Ownership and Data Sovereignty

Its popularity has raised certain questions and given them more attention than was given in the past — not the least that technology we create always also follows economic constraints and has influence on society. But also about the question of data ownership and sovereignty. Blockchains made it very clear that for the most part users aren't fully in control over their data, not even their accounts in the Web2 world. There is no turning back from knowing that.

Open, auditable Infrastructure

Similarly and crucial to ensuring real ownership, all widely adopted Blockchains and decentralized infrastructure have Open Source or at least publicly auditable code bases — as the core idea of "trustlessness" can only be achieved if (theoretically) anyone can also verify that it doesn't do anything than it says. Not only that but also a transparent build process with as many guard rails and proofs as feasible has become common place and no public infrastructure can argue against any of that any more[17].

This includes principles like "build in public" and the publication of white papers (such as this) to make the goals, ideas and motivations transparent and understood.

Smart Contracts

Another key aspect that got wide adoption through Ethereum is the concept of reusable user-generated (and managed) micro-programs that run within a constrained subset of the application and can be verified to be correct by all participants-generally referred to as smart-contracts. The ability of ethereum to allow anyone to upload their own code extensions to the system, build apps on it, that anyone can interact with, was a key driver behind the crypto explosion. NFTs are nothing else than a smart contract on the blockchain.

[17] The german CoronaWarnApp has been built as an OpenSource App for increased trust for that exact reason.

Web2.5

While blockchains took over the mass media, the rest of the world didn't stop turning though. We have an entire sub section just about how social media has changed in the same time frame. The same is true for the devices we use to connect to the internet: when the bitcoin white paper came out the first iPhone was just a year old—Nokia still had the majority market share on mobile devices. Fast forward 15 years and there are over 6.4 billion smartphones in the world[18] now, generating over half of all internet surfing traffic (and increasing)[19].

While, as so often, the countries that had computers first are slowly adapting to this, in many poorer countries they jumped over that step: the smartphone is the first (and only) internet capable device a person owns. That's why the step from user-generated-content website to mobile-first website or app is sometimes coined as the web2.5: the "always on, the go web". In today's world, whatever wants to be successful for the majority of people (in a non-work context) needs to be mobile-first.

Funnily enough, as Blockchain/Web3 took off during the time that upcoming industry missed most of that progress there—it stayed an afterthought: No blockchain out there is mobile-first, very few are even capable of moving the "trustlessness"-aspects over from the full-client into a mobile device. We discussed most of the reasons for that above. On mobile devices, which are the majority of internet devices today, decentralization has not happened.

A glimpse at Web5

Out of these two thoughts emerges the kindle that is Web5: bridging the user centric approach of web2 and 2.5 into a decentralized, crypto-ensured Web5 world. As the entire movement is pretty young there are competing definitions of Web5, which aspects it contains and which are merely optional. For once, the definition Jack Dorsey uses in his pitch deck[20] only talks about federated nodes (without any

[18] https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide
[19] https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet
[20] https://bestpitchdeck.com/tbd

blockchain), but with sovereignty around the identity lying with user via DID[21]s and cryptographic verification in a clearly mobile-first scenario: elevating the "PWA[22] to a DWA[23]".

Other definitions boil it down to: a user-friendly web3 but without all that finance stuff.

Conclusion

On the surface both definitions of Web5 sound like sufficient approaches to tackle some of the problems and challenges we've outlined above. However, as we will see in the next part, the devil is in the details and it isn't quite so simple if you don't first move away from the thinking of a siloed web2 world.

[21] https://www.w3.org/TR/did-core/
[22] PWA: Progressive Web App, see https://en.wikipedia.org/wiki/Progressive_web_app
[23] DWA: Decentralized Web Application

State of the union

From our outline above it should become evident that we don't think current technology, nor the way that major projects are heading at the moment will be sufficient to take on the challenges ahead. However, when talking about these challenges some projects are often mentioned as solutions to it. In this section we want to briefly cover the main upcomers and the problems we see with them.

This is neither a comprehensive list nor does it attempt to cover the entire market, it is a subjective set we have picked. Most notably we have left out any project that never made it out of a niche adoption circle nor generated enough buzz to be asked about. You might consider "popularity" a bad indicator for a technical solution, but we have the perspective that this isn't merely a technical problem and as such "usage adoption" and "mass acceptance" are important indicators indeed. Furthermore we are actively ignoring any project that is proprietary or relies on centralized servers or single-entity owned infrastructure.

Mastodon, Fediverse

The old kids on the block, and since the Twitter meltdown of Nov 2022 well-known, Mastodon is a decentralized, federated alternative to twitter. Based on the so-called "Fediverse", or more precisely the ActivityPub specs[24], everyone can set up their own Mastodon Server and host it for themselves or others. Through the federation mechanisms of ActivityPub any server can connect to and exchange the posts, called toots, with one another without any restrictions or central routing mechanism. The most popular Web-UI, as well as most clients, are mostly trying to mimic twitter, though alternative approaches exist.

Though created in 2016, and the final RFC landing in 2018, cryptographic security is mostly absent from the Fedivers. Most "decentralization" and security is based around the federation and the host-your-own-approach. That, however, heavily piggy-backs on DNS and as the RFC doesn't even mention TLS (or certificate pinning) rendering it vulnerable to DNS-spoofing as well as government or

[24] https://www.w3.org/TR/activitypub/

ISP-driven rerouting. It also doesn't have any fallback, like proxy-routing or similar mechanism in place for that scenario.

Status.IM

In the early days of Ethereum 1.0, there was a chat protocol that piggy-backed on that network: Status.IM used the transaction ethereum gossip protocol called "Whisper" to provide end-user real-live chat. Today's Status Messenger runs on waku, a libp2p-based publish-subscribe protocol, with its own server infrastructure - though technically any libp2p-compatible client could run it, including Eth2 or Polkadot.

What makes Status.IM particularly interesting is that it uses libp2p and crypto to the fullest, thus allowing for local-area discovery through the libp2p-rendezvous-protocol. Thus rendering it the only project in this list capable of being used securely without any ISP connection. The problem of messages in libp2p pub-sub only being available for a short-time has also been elegantly addressed with the concept of mail-servers that receive and store data on your behalf, and as they are encrypted without any privacy concerns.

The messenger itself is a nice, pretty usable mobile App, yet its roots come through hard: many of its features are hard-tied to Ethereum, e.g. ENS-lookup, sending eth within a chat, or it also being a full Ethereum Wallet—mixing chat and money in a slightly uncomfortable way. Considering the current stance of Web3/Blockchains/Cryptography in the public eye, it is unlikely to receive mass adoption any time soon, unless they moved off from that and towards a less Ethereum-attached App, which, considering the teams background, seems unlikely to happen any time soon.

Blue Sky's @ Protocol

When Jack Dorsey left Twitter he announced that his new Company, TBD[25], would be working on a decentralized alternative to Twitter, called BlueSky. Little was known about the actual concept of it during its research phase. A of late October

[25] Actual name of the company

2022[26] and the publication of the first set of design documentation we know a little more:

The At-Protocol, as the underlying technology is called, has a heavy focus on algorithmic choice and account portability. The latter is supposed to be made possible through DIDs[27] which should be looked up in the DNS-entry of the user's domain[28].

Aside from facing the same issue as the Fediverse, that the majority of people is probably not actually fully sovereign but will (have to) just use someone else's server, this, too, requires DNS to be available for lookup. Despite that content otherwise is meant to be signed cryptographically, any actual private end-to-end-encrypted communication is nowhere to be found in its documentation. Similarly, the lack of any peer-to-peer or forwarding mechanism is disappointing considering that the underlying IPLD data structures are taken from the fully peer-to-peer IPFS-network, which had these for years.

Matrix.org

The chat interoperability network that Blue Sky seemingly drew inspiration from (next to Dat, IPFS and Mastodon/Fediverse) and it still uses to host its developer channel (at least the public part) is the Matrix Protocol.

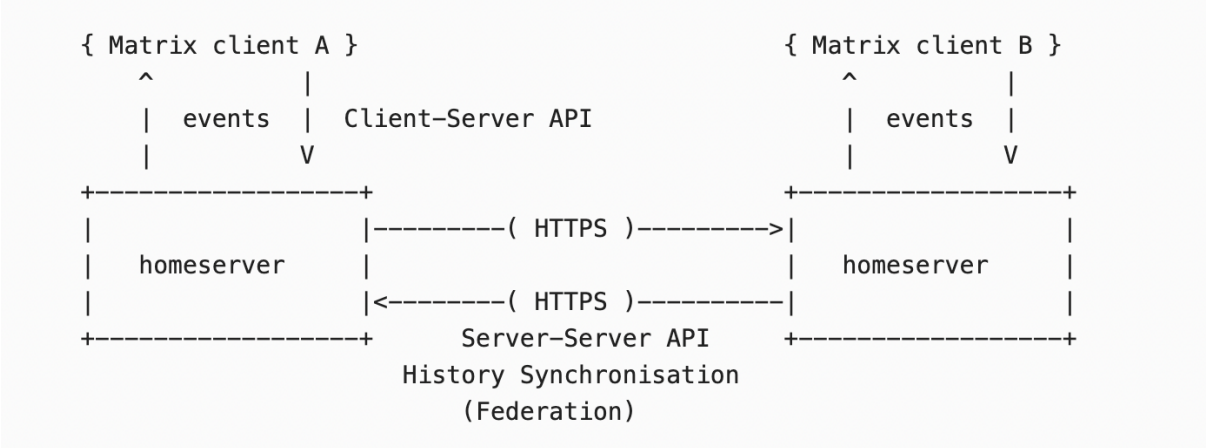
Similar to Status.IM, Matrix.org is an open spec protocol for chat—though Matrix has been around much longer and comes from a different background: Matrix' original goal was to break up the silos of the modern messenger world. That explains why from its earliest DNA matrix is not only federated it expects information to be bridged into the network (and out to others). Making this a pretty unique protocol to begin with: it doesn't act as if it was the only network around, it accepts the world in which some people you want to talk to do not have a client speaking the protocol natively but want to communicate over a different protocol.

---

[26] https://blueskyweb.xyz/blog/10-18-2022-the-at-protocol
[27] https://www.w3.org/TR/did-core/
[28] This is a vast simplification, as the at-protocol also offers non-dns-based alternatives, but realistically and practically, and considering the amount the docs spent on it, these are not really expected to play a real role.

This doesn’t come without its challenges though: Full end-2-end-encryption is pretty hard if you want to bridge over into networks that don’t support it or support other forms of encryption. Matrix itself is a federated end-2-end-encryption protocol with a variety of clients and some server implementations. What makes the project particularly interesting for us, is its structural nature: messages are encoded as JSON and attached to rooms, with some special messages altering the room's state (think avatar or name of the room, but also permissions). In order to ensure the state comes up the same on all federated nodes (only those server, who joined a room, are actually receiving the messages for it) the messages are calculated as a directed acyclic graph (DAG)[29] and thus a deterministic order of events is ensured. At its core Matrix is an event stream with deterministic order sent by its clients.

If that sounds familiar to you it probably is from the blockchain world. Unlike a blockchain network where the entire network is working on one singular global chain representing the state in Matrix every room is effectively its own little blockchain. The network distributes messages between the room's participants only, rendering it a much more efficient state management mechanism. On top, it allows for end-to-end-encrypted message transfer, which most blockchains can not account for.



The Matrix architecture today. Source: matrix.org

---

29 https://matrix.org/blog/2020/06/16/matrix-decomposition-an-independent-academic-analysis-of-matrix-state-resolution

That said, there is still quite a bit of way to go: Same as for Mastodon a lot of responsibility is given to the federation nodes in the network, called homeserver: for many messages in the network, not the user signature is required but the signature of the homeserver. Thus, users are bound to their homeserver, which is not bound to DNS by the spec, but for now in practice. A peer-to-peer implementation with a fully decentralized DNS-less homeserver is in the works[30]. Yet there remains work to be done in particular regarding cryptographic security of user messages and support for DNS-less environments.

Conclusion

From this little overview we can see the technology is almost there. But the focus of these projects leaves one wondering if they are able to adapt for the upcoming challenges: to truly become an application platform the average user can rely on and use easily. The most promising, in the eyes of the authors, is Matrix. Even though it might seem farther away than e.g. Status: its transparent protocol spec process, open extensible data format yet stable and promising scaling mechanisms through distributing along rooms make for a great starting point.

[30] https://arewep2pyet.com/

Endnotes

You can follow the project at: **effektio.org**
On twitter as: @effektio
On matrix at: #news:effektio.org
On Mastodon at: effektio@effektio.org
The Newsletter at: effektio.org/newsletter
On Github at: effektio/effektio
The current dev docs at: docs.effektio.org

You can contact the team directly via
Via email at: team@effektio.org
On Matrix in: #foyer:effektio.org

If you have specific questions or remarks, feel free to write the authors directly at whitepaper@effektio.org or use the commenting function google provides here.

Changelog

We follow Semantic Versioning for this document in the format Major.Minor.Patch. Where patch changes are only changes without any further meaning, such as fixes of typos or clarifications; Minor signals a significant addition or change in the understanding or focus and Major signals a fundamental next iteration of the entire architecture and ideas of the document.

Version	*Release Date*	*Changes*
1.0.0	2022-12-06	Initial Release