CryptPad

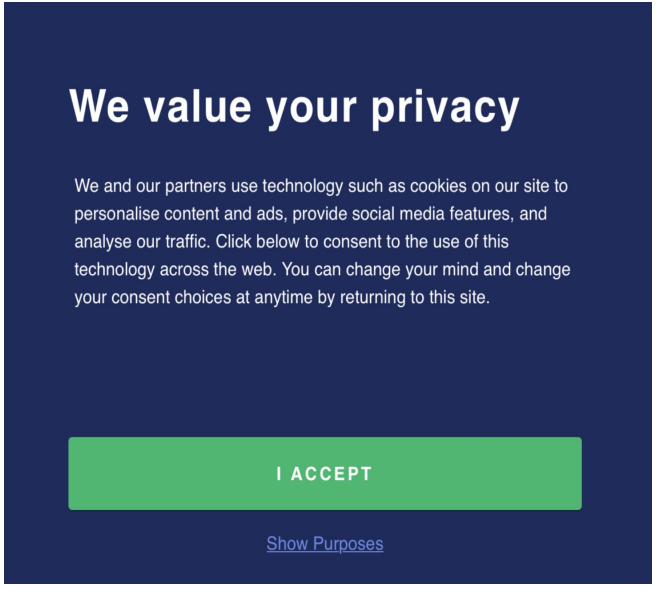
The Encrypted Collaboration Suite

Who am I ?

- Ludovic Dubost, CEO of XWiki SAS
- Creator of XWiki - Enterprise Wiki
- 15 years of Open Source
- 40 employees: "make a living & contribute"
- XWiki SAS launched CryptPad as a new tool 4 years ago

Why CryptPad ?

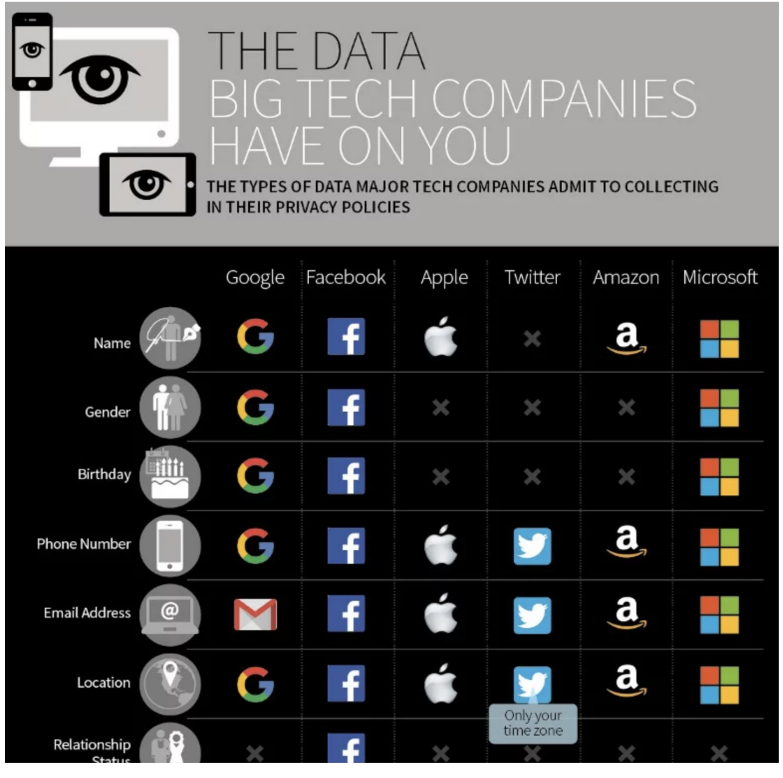
What they say ?

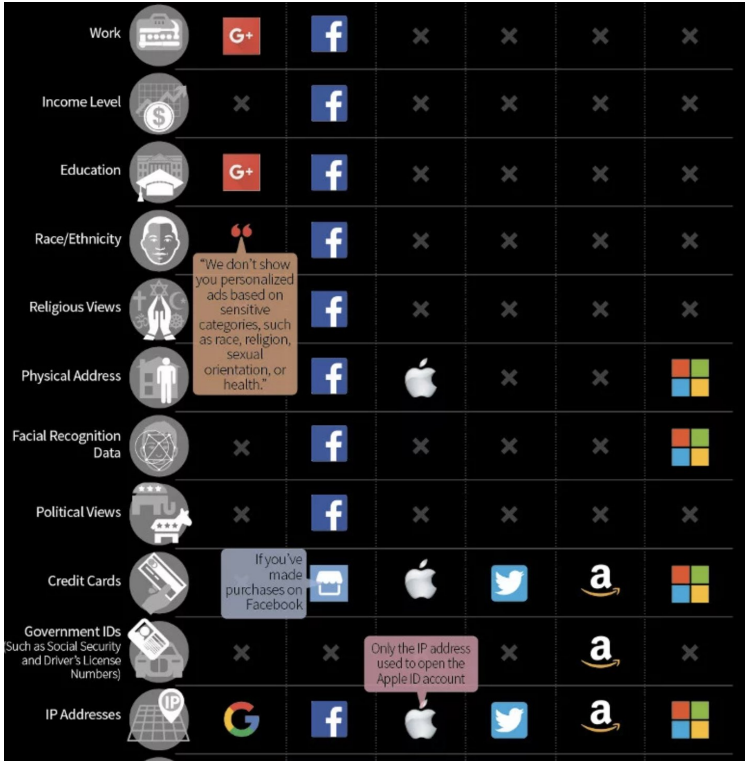


What they mean

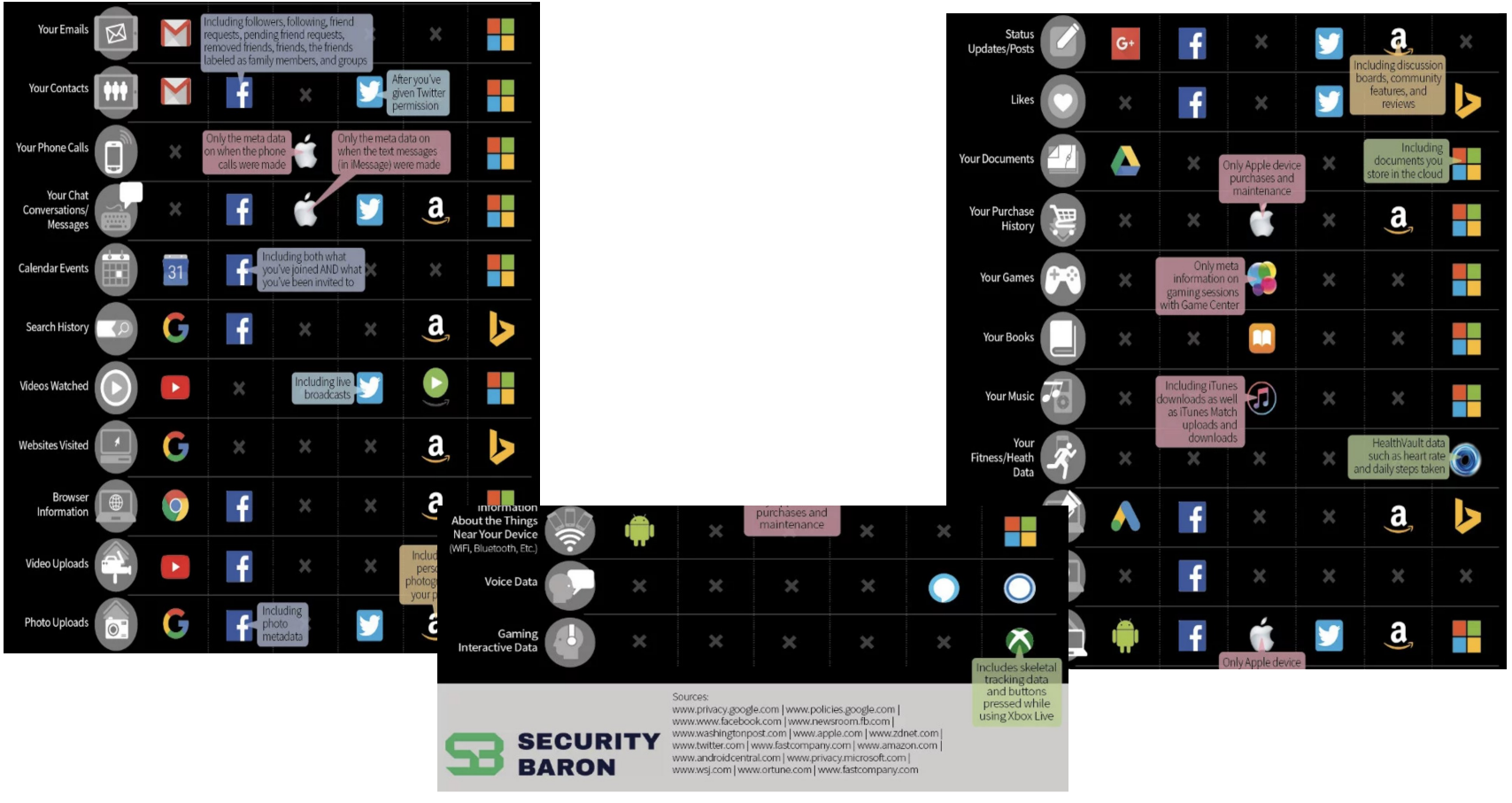
We use & sell your data

What Big Tech knows: a long list





… a very long list



What about security ?

- Our data is unencrypted everywhere
- Transparency is very low
- Small actors and individuals have a hard time securing data

Why CryptPad ?

- Could we actually enforce user's privacy & security using encryption ?
- Alternative to collaboration tools (Google Drive, Dropbox, Trello) guided by privacy & security principle
- No business model based on user's data

CryptPad - Key principles

- Creating encrypted shared documents that can be edited in real time
- Manage keys of shared documents in personal, shared or team drives
- Exchange keys using personal messaging boxes using public/private key cryptography

What does CryptPad know about you

Things we cannot avoid to see but do not collect

- IPs and Public Key

Things we store because we need it

- Encrypted Files, linked to users
- Identity when being a paying user
- Statistical information (including location)

What we can't know

- Your password
- Your username
- The content including text, title, structured data, names of collaborators

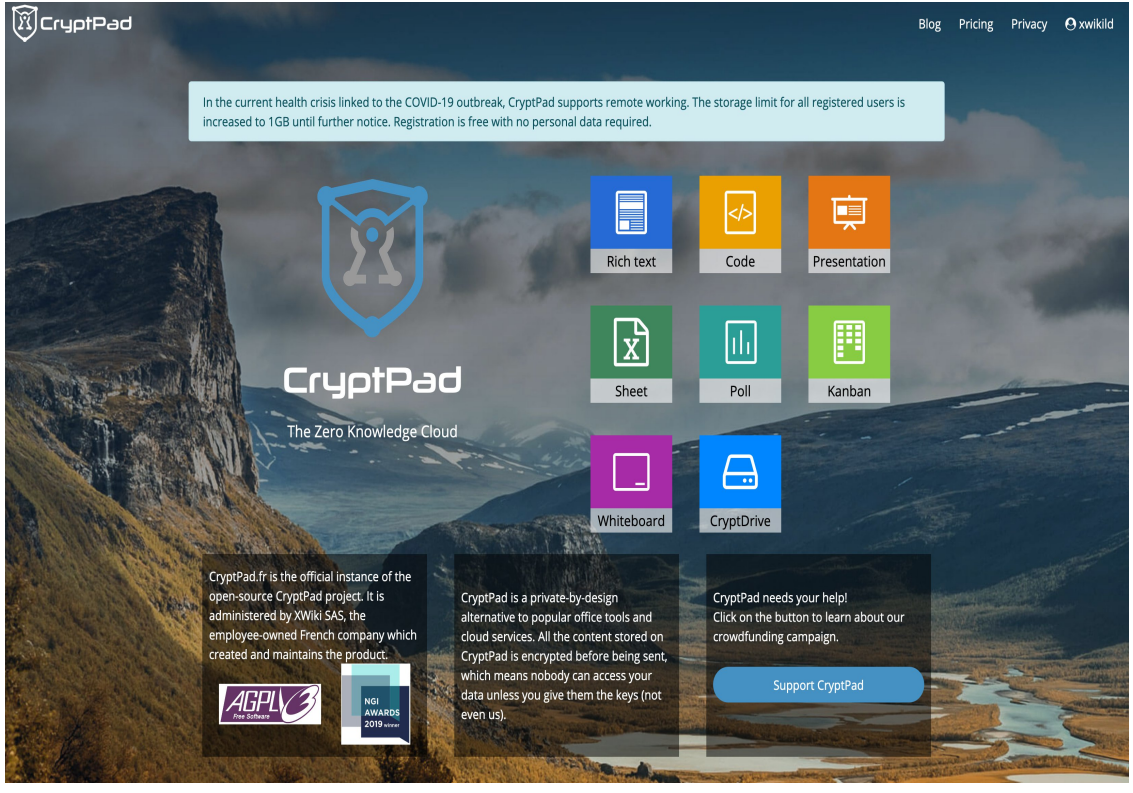
CryptPad: what do we have ?

- Many pad types:
  - RichText / Wysiwyg (HTML)
  - Code (Markdown)
  - Presentation (Markdown)
  - Sheets (Excel compatible / OnlyOffice)
  - Kanban
  - Whiteboard
  - Poll
- CryptDrive
- Teams

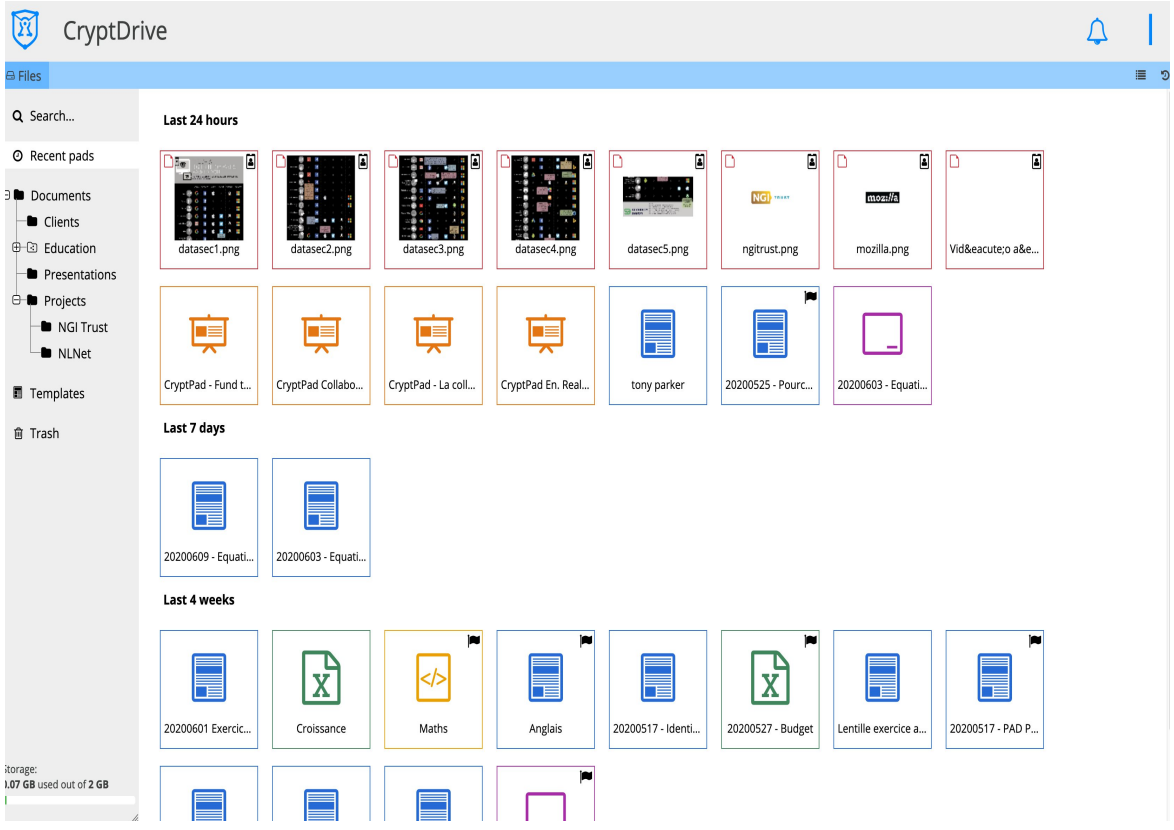
CryptPad: Privacy by design

Live demo of a few features

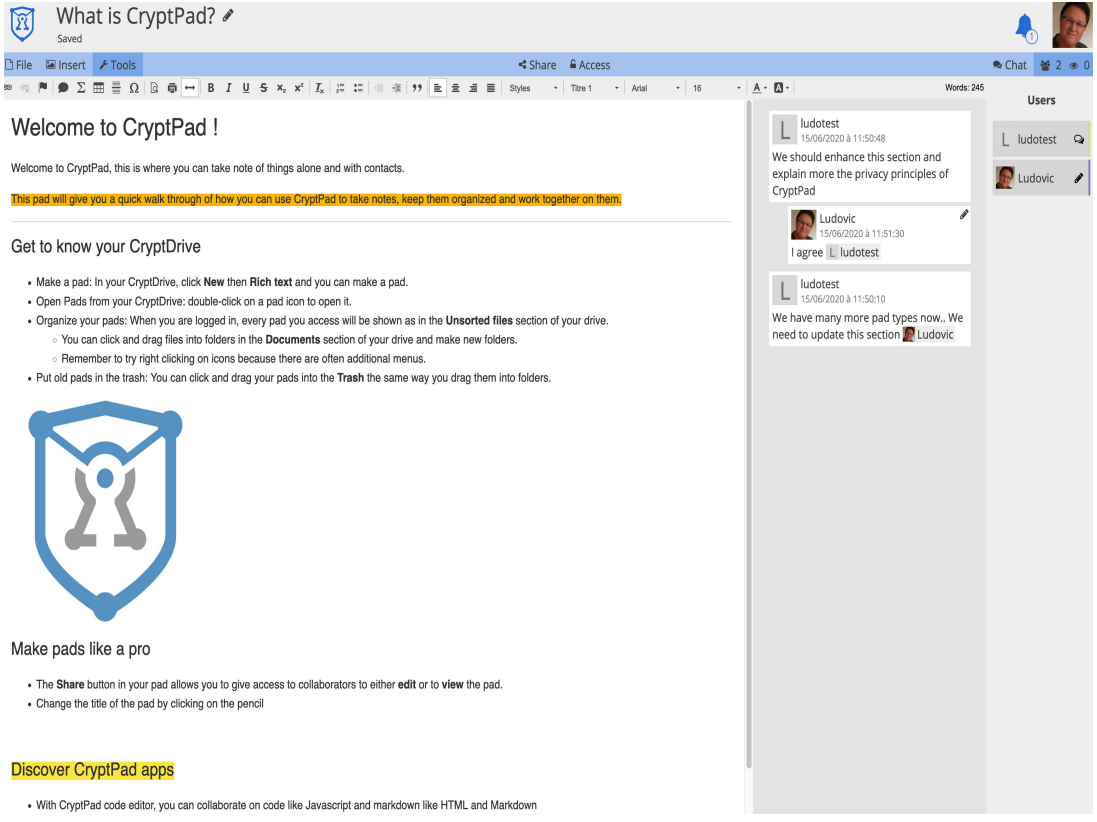
CryptPad: Demo



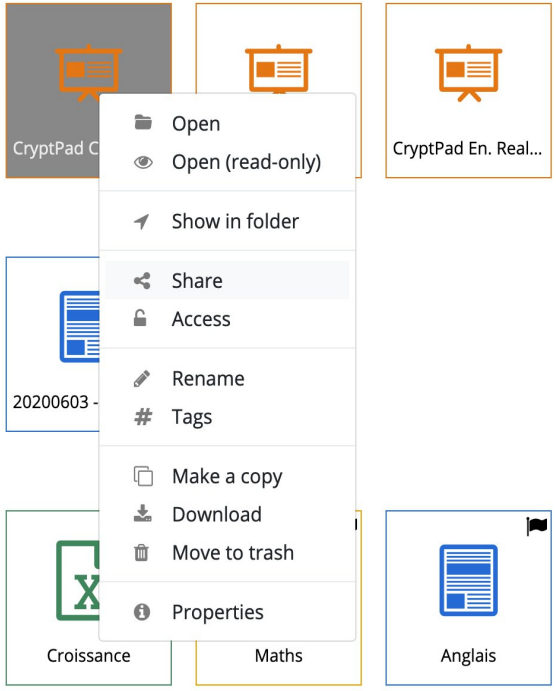
CryptPad: Demo

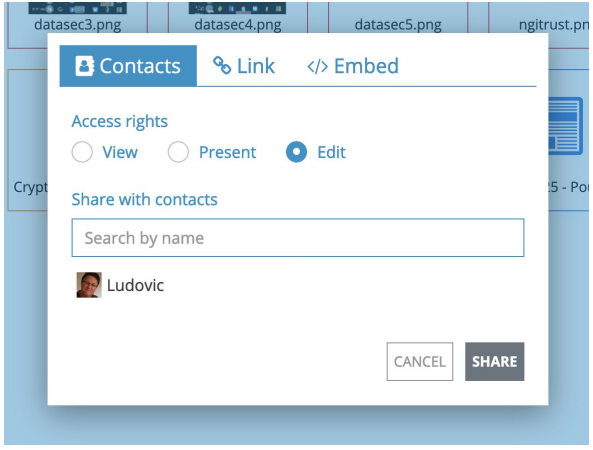


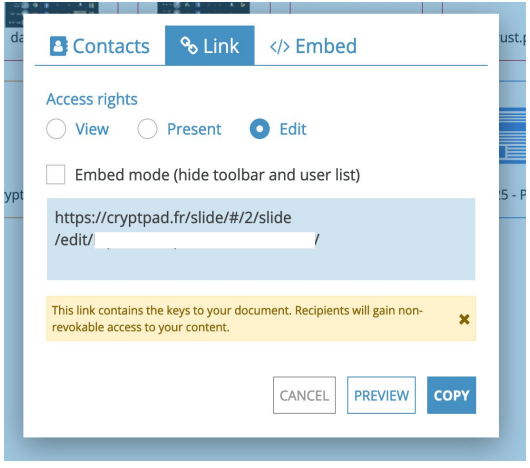
CryptPad: Demo



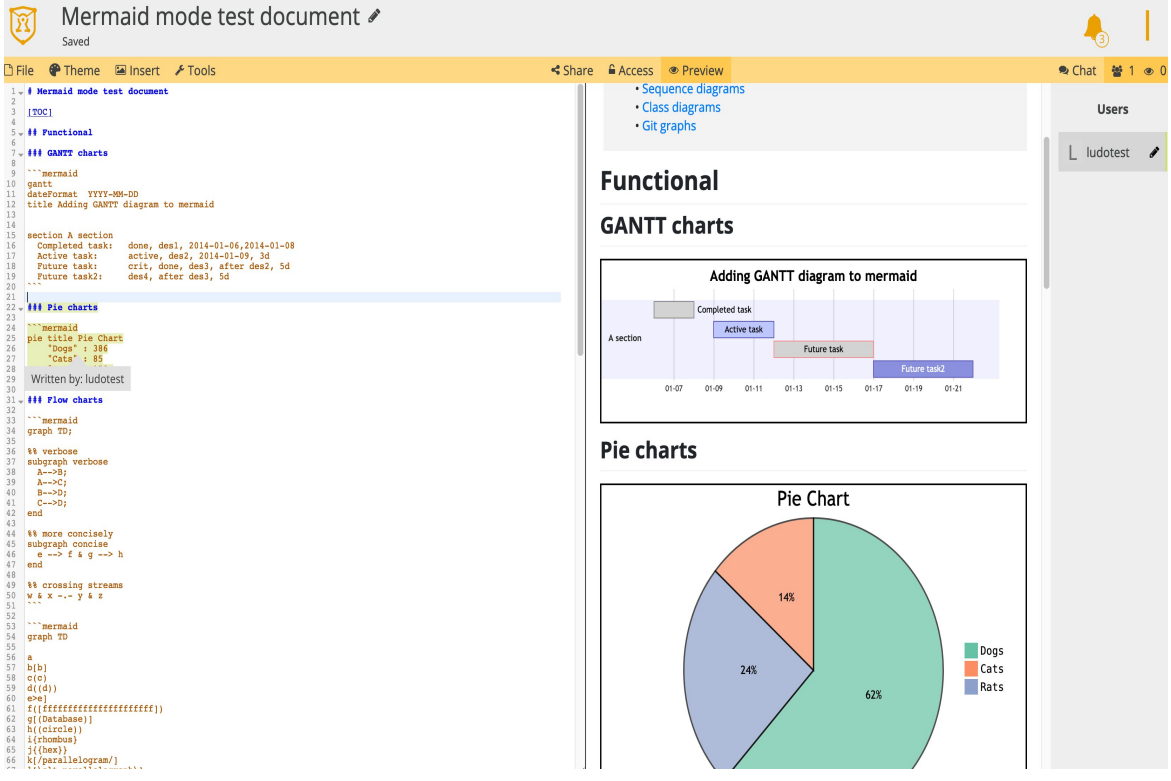
CryptPad: Demo



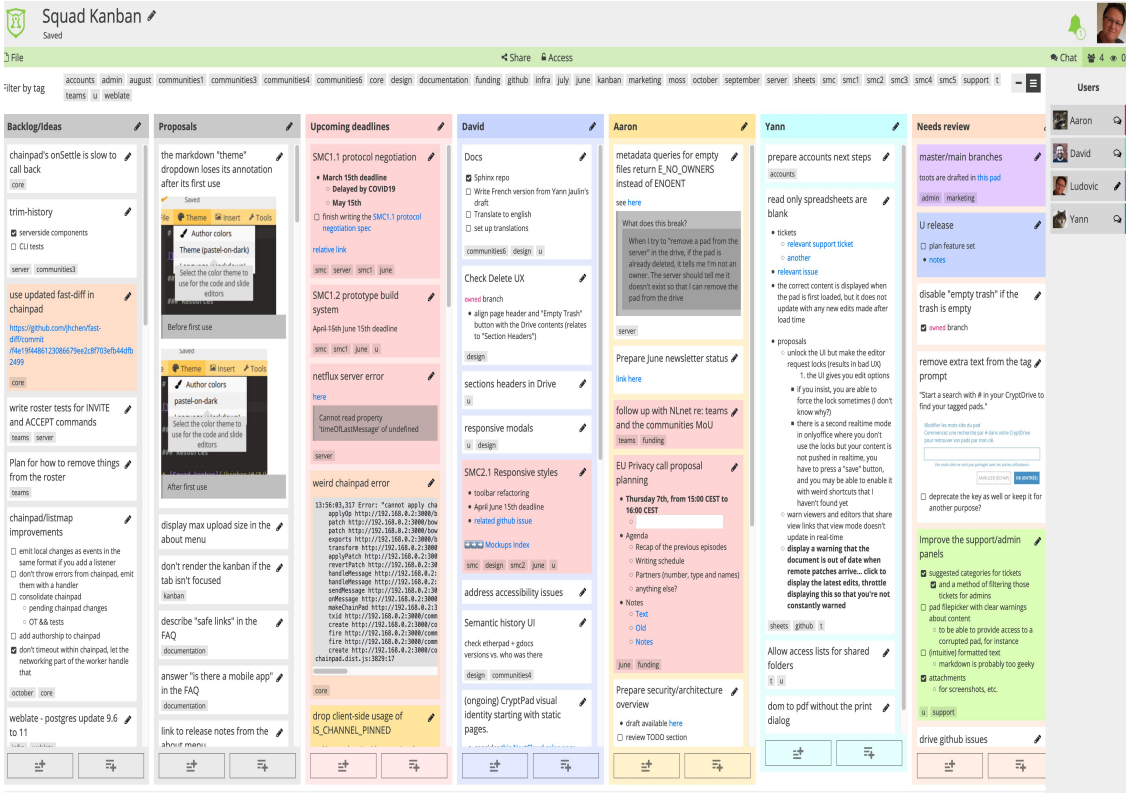




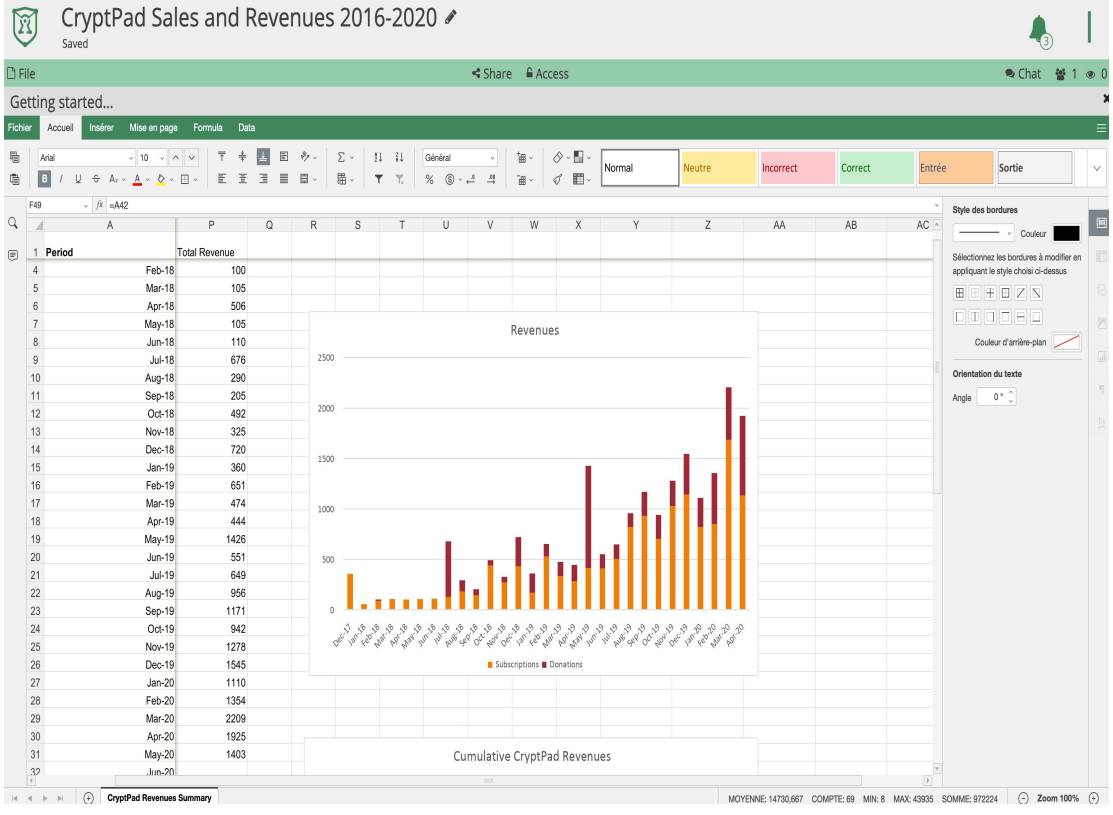
CryptPad: Demo



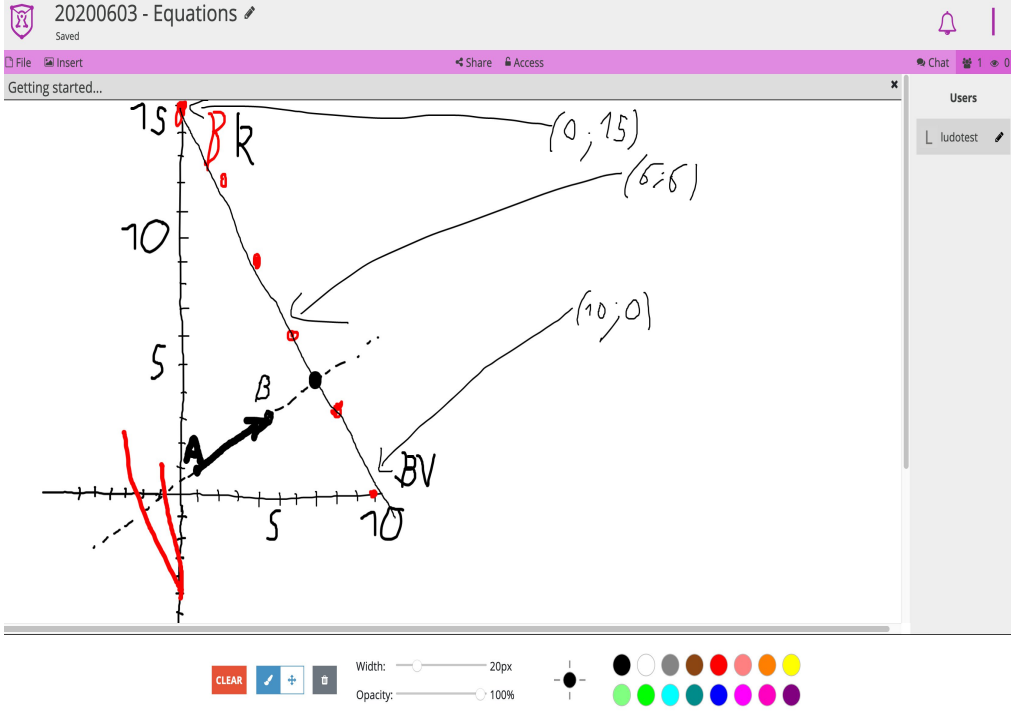
CryptPad: Demo



CryptPad: Demo



CryptPad: Demo



CryptPad: Technological aspects

- User authentication: username & password do not leave the user's computer (using scrypt)
- CryptPad encrypts document changes (patches) and sends them to the server
- ChainPad algorithm allows to handle concurrent changes without the server being involved

CryptPad: Technological aspects

- CryptPad documents are stored as a history of patches. Checkpoints with the full document are saved every 50 patches
- The document encryption keys are stored in your drive which is a CryptPad document itself
- Editors are fully written in Javascript with no server component

CryptPad: How far can this go ?

- Many document editors built in Javascript could be ported to CryptPad encrypted storage (OnlyOffice, Draw.io, Mindmaps, etc...)
- More advanced applications could be build on top of the CryptPad encrypted storage (Calendars, Blogs, Wikis, Forms/Databases, Surveys)
- Encrypted audio/video conferencing

CryptPad: How far can this go ?

- But there is a lot of work to bring editors or application on par with non encrypted applications
- Mobile & Offline require significant work
- More advanced Search is also requiring work
- Decentralization is possible

Roadmap - next 6 months

Communities project (**NLNet NGI Zero**):

- Finishing project
- Improved document review
- Administration panel
- Documentation for users and instances administrators

SMC - Secure Mobile Communication (NGI Trust):

- Developping a prototype Android application

Dialogue Project (NLNet NGI Zero):

- Improve the current Poll application and implement a Form application

Maintenance & Performance

cryptpad.fr usage

COVID Work from Home + School spike

Heavy usage in Germany

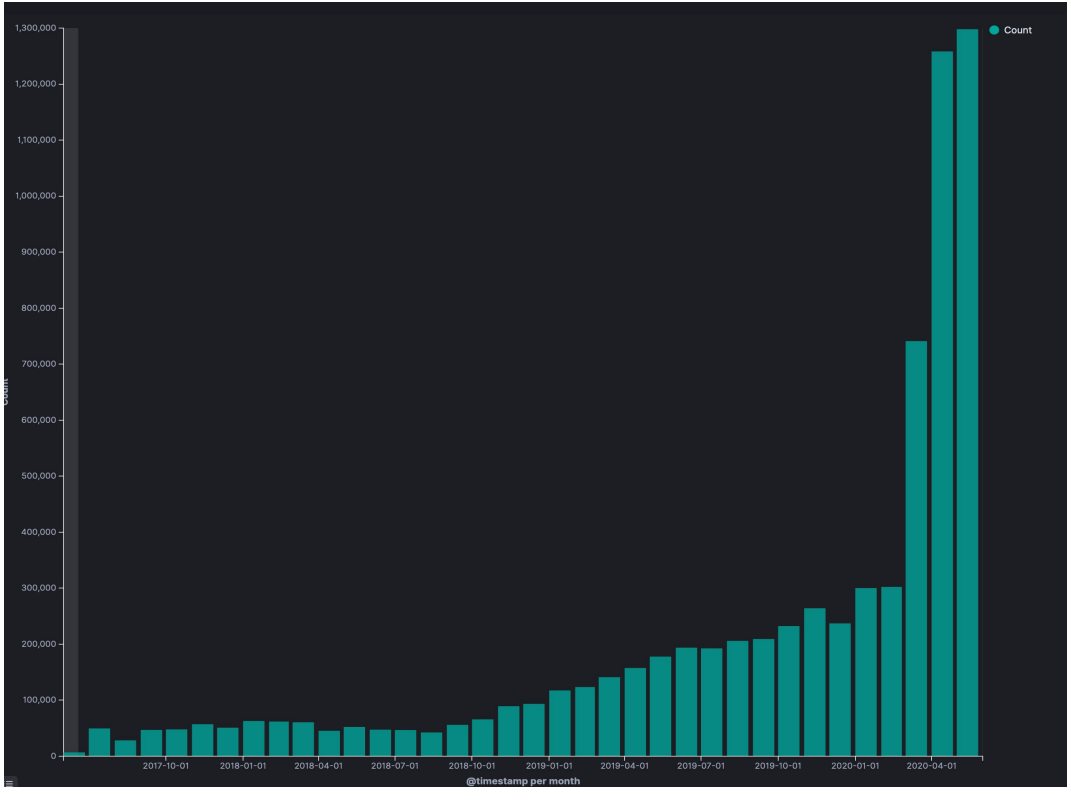
50000+ users per week

350000+ pads open per week

450 installs

Spike in the USA

cryptpad.fr usage



From 150k pads a month to 1.3 Million in a year
Many of our users have recommended CryptPad !

CryptPad Team

- 3 full-time developers at XWiki SAS handling the development and the main cryptpad.fr instance
- (Some) support of the XWiki SAS team (HR, Marketing, me)
- 400+ independent instances
- Community users helping out administrators and helping promoting

CryptPad Funding

- European Community
  - Thank you NLNet - NGI PET ZERO ! (150KEuros)
  - Thank you NGI Trust (70KEuros)
- Mozilla Open Source Fund (10K$)
- BPI France (Initial research funding)

CryptPad Long Term Funding

- 170+ subscribers of CryptPad.fr
(1000 Euros / month)

- 160+ Donators on OpenCollective
(500 Euros / month)

20KEuros for 2020

Still **10x away** being able to fund a team only based on revenue