



CryptPad

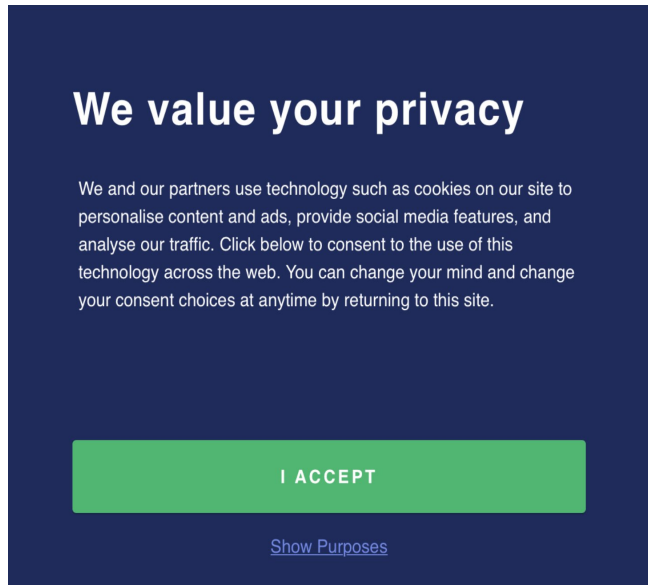
**The Encrypted
Collaboration Suite**

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

 THE DATA BIG TECH COMPANIES HAVE ON YOU
THE TYPES OF DATA MAJOR TECH COMPANIES ADMIT TO COLLECTING IN THEIR PRIVACY POLICIES

	Google	Facebook	Apple	Twitter	Amazon	Microsoft
Name				×		
Gender			×	×	×	
Birthday			×	×	×	
Phone Number						
Email Address						
Location						
Relationship Status	×		×	×	×	×

Only your time zone

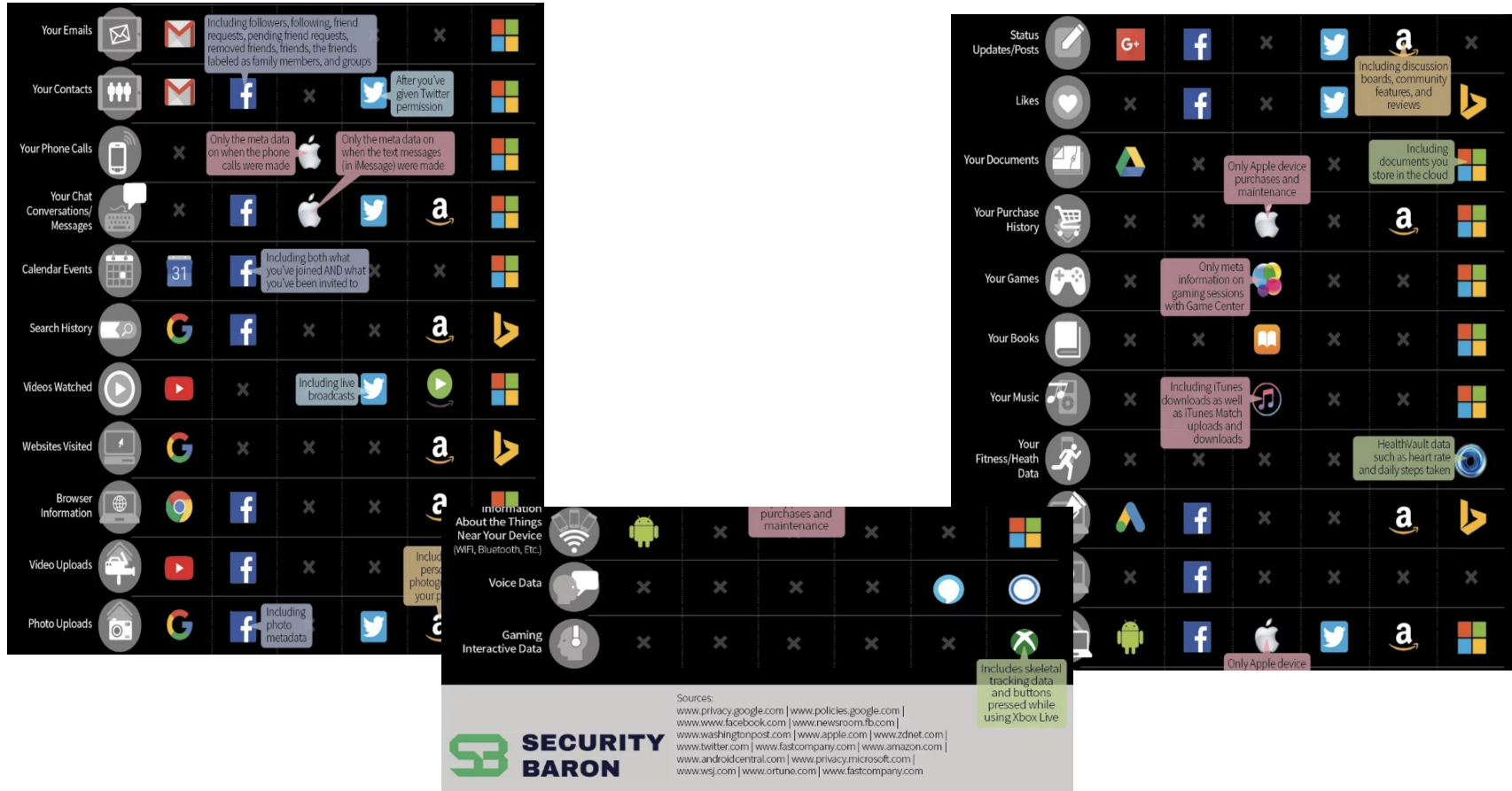
Work			×	×	×	×
Income Level	×		×	×	×	×
Education			×	×	×	×
Race/Ethnicity	×		×	×	×	×
Religious Views	×		×	×	×	×
Physical Address	×			×	×	
Facial Recognition Data	×		×	×	×	
Political Views	×		×	×	×	×
Credit Cards	×					
Government IDs Such as Social Security and Driver's License Numbers	×	×	×	×		×
IP Addresses						

"We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health."

If you've made purchases on Facebook

Only the IP address used to open the Apple ID account

... 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

The image shows a screenshot of the CryptPad website. The background is a scenic landscape with mountains and a river. The website has a dark blue header with the CryptPad logo on the left and links for 'Blog', 'Pricing', 'Privacy', and 'xwikild' on the right. A light blue banner at the top contains a message about COVID-19. The main content area features the CryptPad logo and tagline 'The Zero Knowledge Cloud'. To the right of the logo is a grid of nine colored squares, each with an icon and a label: 'Rich text' (blue), 'Code' (orange), 'Presentation' (orange), 'Sheet' (green), 'Poll' (teal), 'Kanban' (light green), 'Whiteboard' (purple), and 'CryptDrive' (blue). Below the grid are three dark blue boxes with white text. The first box on the left describes CryptPad.fr as the official instance of the open-source project, administered by XWiki SAS. The middle box describes CryptPad as a private-by-design alternative to office tools. The right box asks for support and includes a 'Support CryptPad' button. At the bottom left, there are two award logos: 'AGPL 3' and 'NGI AWARDS 2019'.

CryptPad: Demo

The screenshot displays the CryptDrive web interface. At the top, the header bar includes the CryptDrive logo, a search bar, and a notification bell. Below the header, a sidebar on the left provides navigation options: 'Files', 'Recent pads', 'Documents' (with sub-items 'Clients', 'Education', 'Presentations', 'Projects', 'NGI Trust', 'NLNet'), 'Templates', and 'Trash'. The main content area is organized into three sections based on time: 'Last 24 hours', 'Last 7 days', and 'Last 4 weeks'. Each section contains a grid of file thumbnails. The 'Last 24 hours' section shows several image files (dataset1.png through dataset5.png, ngitrust.png, mozilla.png, and a video file) and four presentation files. The 'Last 7 days' section shows two document files. The 'Last 4 weeks' section shows a variety of files including documents, spreadsheets, and code files. At the bottom left, a storage status indicator shows '1.07 GB used out of 2 GB'.

CryptDrive

Files

Search...

Recent pads

- Documents
 - Clients
 - Education
 - Presentations
 - Projects
 - NGI Trust
 - NLNet
- Templates
- Trash

Last 24 hours

- dataset1.png
- dataset2.png
- dataset3.png
- dataset4.png
- dataset5.png
- ngitrust.png
- mozilla.png
- Vidéeo a&e...
- CryptPad - Fund t...
- CryptPad Collabo...
- CryptPad - La coll...
- CryptPad En. Real...
- tony parker
- 20200525 - Pourc...
- 20200603 - Equati...

Last 7 days



- 20200609 - Equati...
- 20200603 - Equati...

Last 4 weeks



- 20200601 Exercic...
- Croissance
- Maths
- Anglais
- 20200517 - Identi...
- 20200527 - Budget
- Lentille exercice a...
- 20200517 - PAD P...

Storage: 1.07 GB used out of 2 GB

CryptPad: Demo

What is CryptPad? 

Saved

FileInsertTools

ShareAccess

Chat20

FileInsertTools

ShareAccess

Chat20

Words: 245

Users


Welcome to CryptPad !

Welcome to CryptPad, this is where you can take note of things alone and with contacts.

This pad will give you a quick walk through of how you can use CryptPad to take notes, keep them organized and work together on them.

Get to know your CryptDrive

- Make a pad: In your CryptDrive, click **New** then **Rich text** and you can make a pad.
- Open Pads from your CryptDrive: double-click on a pad icon to open it.
- Organize your pads: When you are logged in, every pad you access will be shown as in the **Unsorted files** section of your drive.
 - You can click and drag files into folders in the **Documents** section of your drive and make new folders.
 - Remember to try right clicking on icons because there are often additional menus.
- Put old pads in the trash: You can click and drag your pads into the **Trash** the same way you drag them into folders.




Make pads like a pro


- The **Share** button in your pad allows you to give access to collaborators to either **edit** or to **view** the pad.
- Change the title of the pad by clicking on the pencil


Discover CryptPad apps


- With CryptPad code editor, you can collaborate on code like Javascript and markdown like HTML and Markdown


ludotest
15/06/2020 à 11:50:48


We should enhance this section and explain more the privacy principles of CryptPad


Ludovic
15/06/2020 à 11:51:30


I agree 


ludotest
15/06/2020 à 11:50:10

We have many more pad types now.. We need to update this section 

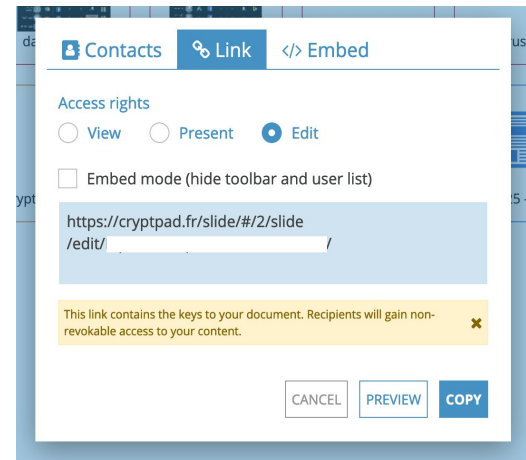
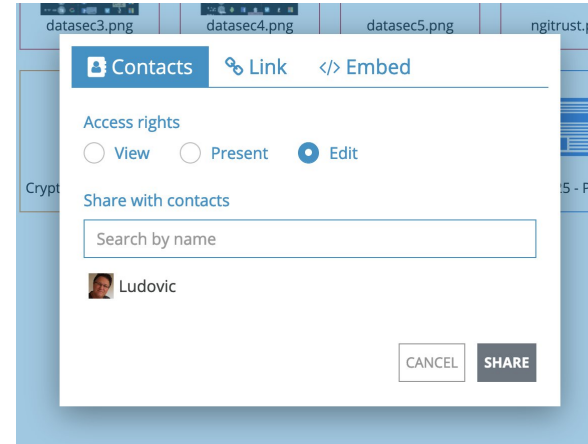
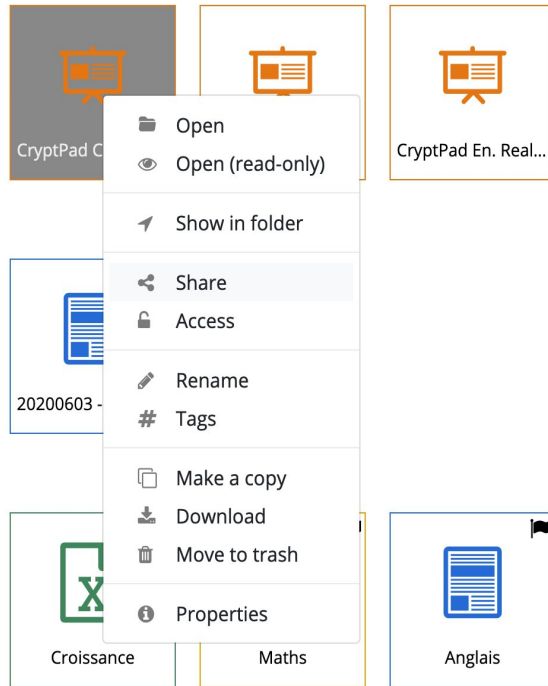
ludotest




Ludovic




CryptPad: Demo



CryptPad: Demo

Mermaid mode test document

Saved

3

FileThemeInsertTools

ShareAccessPreview

Chat10

```
1. Mermaid mode test document
2. [TOC]
3.
4.
5. ## Functional
6.
7. ### GANTT charts
8.
9. ---mermaid
10. gantt
11.   dateFormat YYYY-MM-DD
12.   title Adding GANTT diagram to mermaid
13.
14.
15. section A section
16.   Completed task: done, des1, 2014-01-06,2014-01-08
17.   Active task: active, des2, 2014-01-09, 3d
18.   Future task: crit, done, des3, after des2, 5d
19.   Future task2: des4, after des3, 5d
20. ---
21.
22. ### Pie charts
23.
24. ---mermaid
25. pie title Pie Chart
26.   "Dogs" : 386
27.   "Cats" : 89
28.
29.   Written by: ludotest
30.
31. ### Flow charts
32.
33. ---mermaid
34. graph TD;
35.
36. %% verbose
37. subgraph verbose
38.   A-->B;
39.   A-->C;
40.   B-->D;
41.   C-->D;
42. end
43.
44. %% more concisely
45. subgraph concise
46.   e --> f & g --> h
47. end
48.
49. %% crossing streams
50. w & x -- y & z
51. ---
52.
53. ---mermaid
54. graph TD
55.
56. a
57. b[b]
58. c[c]
59. d[d]
60. e[e]
61. f[fffffffffffffffffffff]
62. g[(database)]
63. h((circle))
64. i(rhombus)
65. j((hex))
66. k[/parallelogram/]
67. ---
68. ---
```

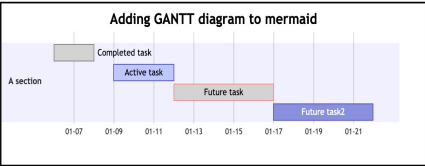
• Sequence diagrams

• Class diagrams

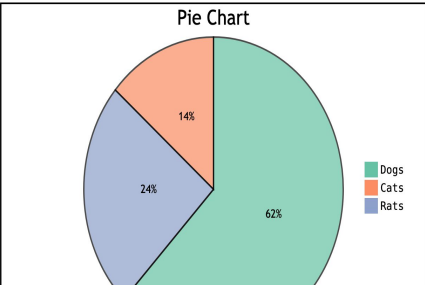
• Git graphs

Functional

GANTT charts



Pie charts



Users

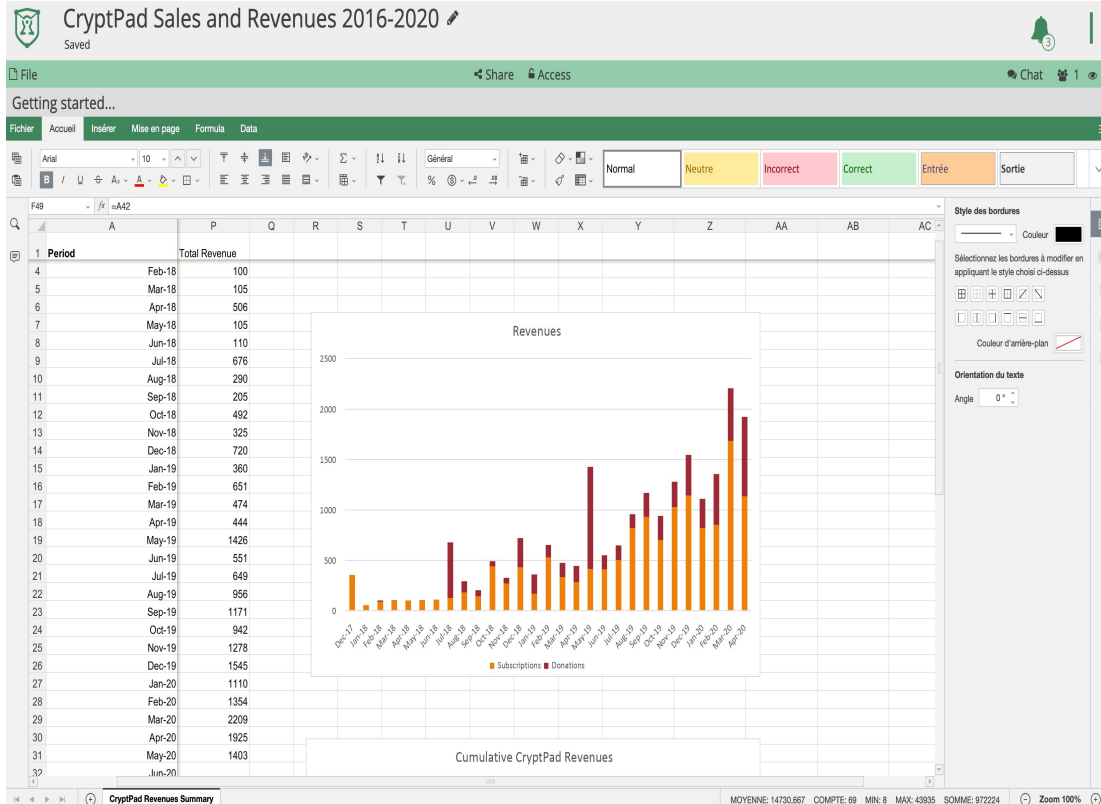
ludotest

CryptPad: Demo

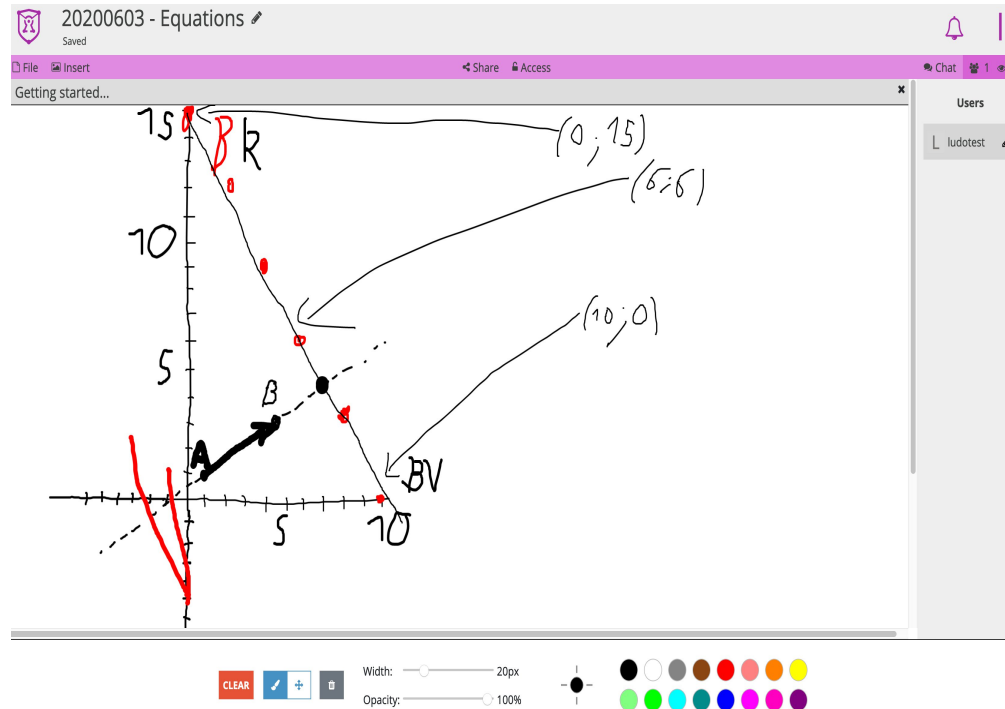
The screenshot displays the CryptPad interface for a project named "Squad Kanban". The interface is organized into several main sections:

- Header:** Includes a "Saved" status, a "Share" button, and a "Access" dropdown menu. A chat window is visible in the top right corner.
- Navigation Bar:** A horizontal bar with tabs for "File", "accounts", "admin", "audit", "communities", "core", "design", "documentation", "funding", "github", "infra", "july", "june", "kanban", "marketing", "moss", "october", "september", "server", "sheets", "smc", "smc1", "smc2", "smc3", "smc4", "support", and "website".
- Main Content Area:** A Kanban board with columns for different stages of work. Each column contains cards representing tasks or documents. The columns are color-coded: Backlog/Ideas (grey), Proposals (orange), Upcoming deadlines (pink), David (blue), Aaron (yellow), Yann (cyan), and Needs review (red).
- Left Sidebar:** A vertical list of tasks and documents, including "chainpad's onSettle is slow to call back", "trim-history", "use updated fast-diff in chainpad", "write roster tests for INVITE and ACCEPT commands", "Plan for how to remove things from the roster", "chainpad/listmap improvements", "describe 'safe links' in the FAQ", "answer 'is there a mobile app' in the FAQ", and "link to release notes from the about menu".
- Right Sidebar:** A vertical list of tasks and documents, including "master/main branches", "U release", "disable 'empty trash' if the trash is empty", "remove extra text from the tag prompt", "improve the support/admin panels", and "drive github issues".

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):

- Developing a prototype Android application

Dialogue Project (NLNet NGI Zero):

- Improve the current Poll application and implement a Form application

Maintenance & Performance

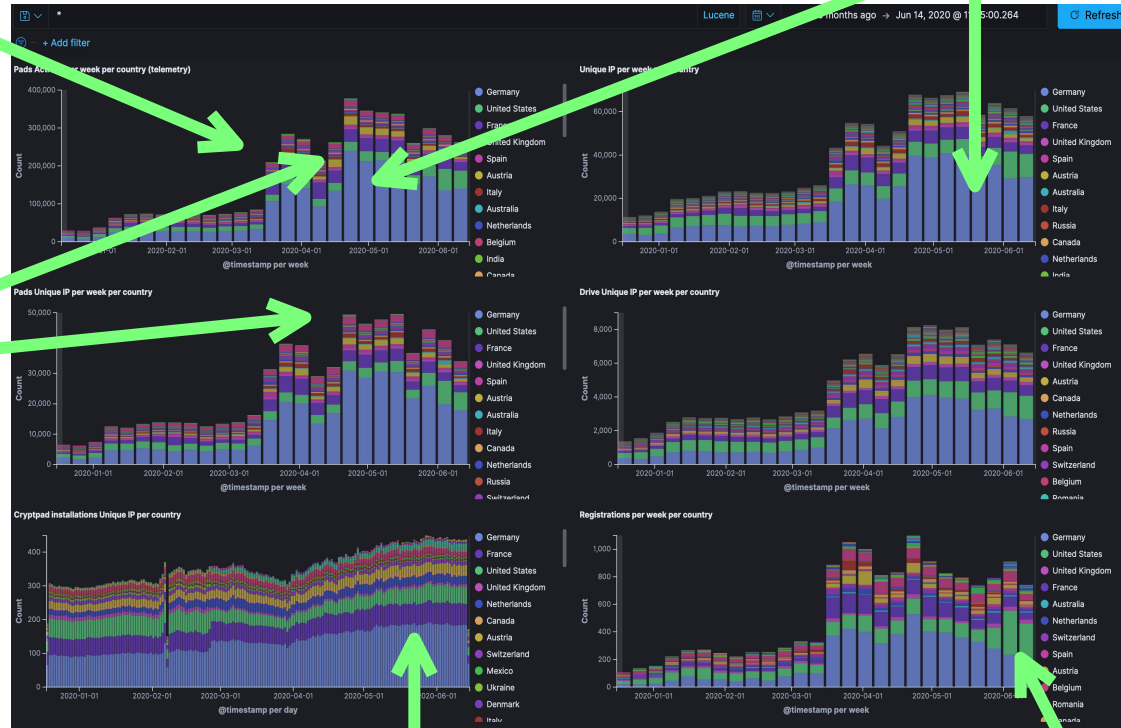
cryptpad.fr usage

COVID Work from Home + School spike

Heavy usage in Germany

50000+ users
per week

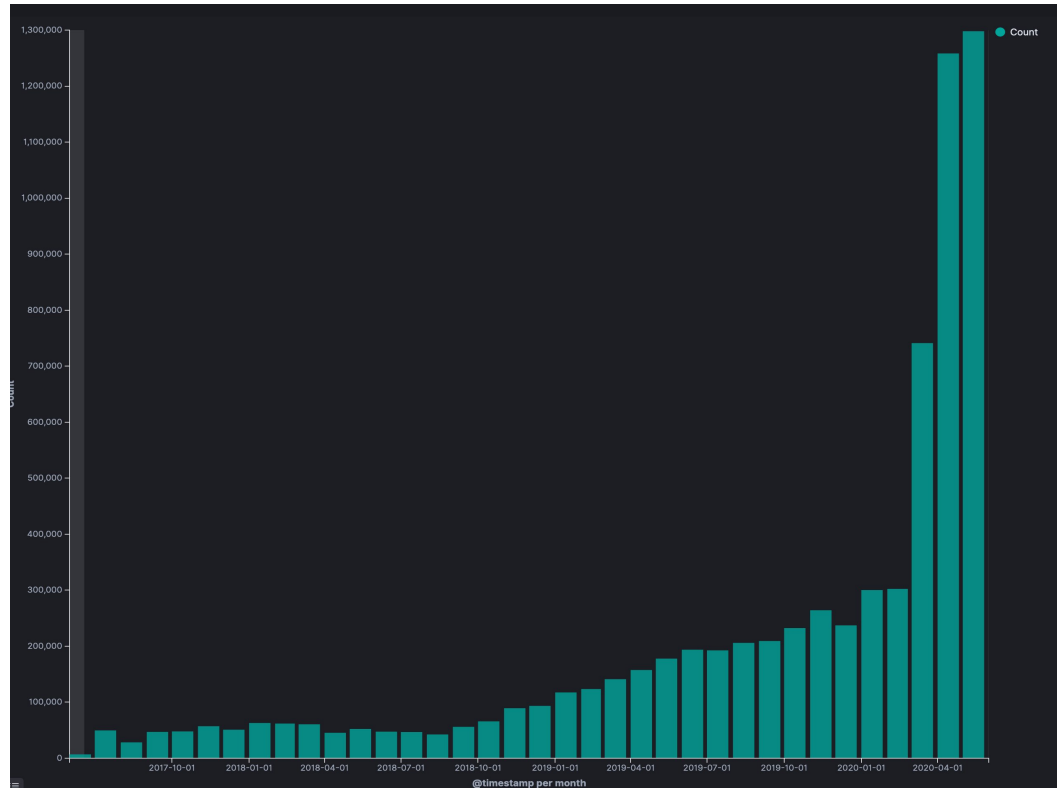
350000+ pads
open per
week



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