



# 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 ?

**We value your privacy**

We and our partners use technology such as cookies on our site to personalise content and ads, provide social media features, and analyse our traffic. Click below to consent to the use of this technology across the web. You can change your mind and change your consent choices at anytime by returning to this site.

**I ACCEPT**

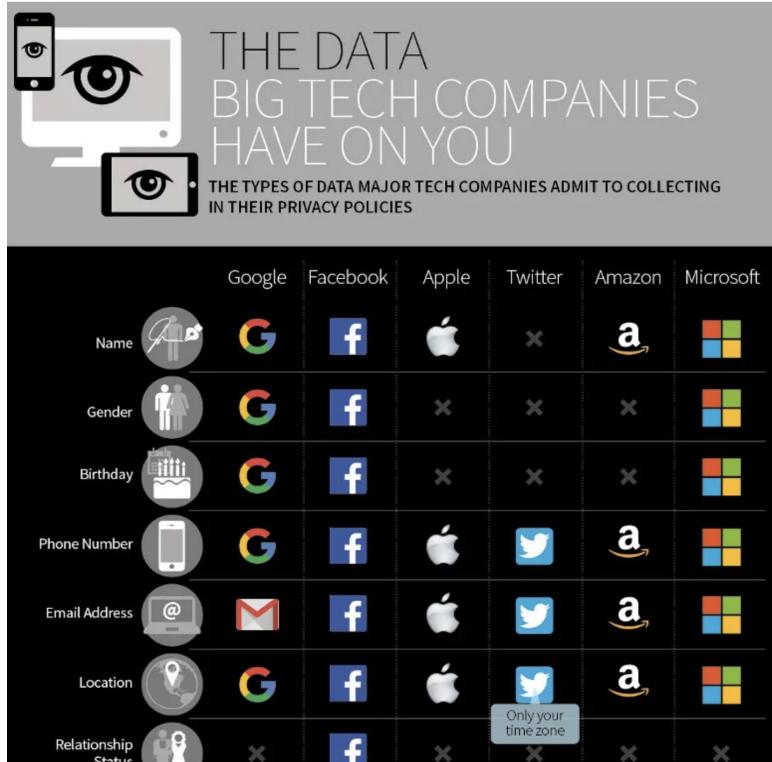
[Show Purposes](#)

## What they mean

We use & sell your data



# What Big Tech knows: a long list



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

# ... a very long list

The chart displays a grid of icons representing different data categories and company logos. A legend at the bottom defines the icons:

- Your Emails:** Includes icons for Gmail, Outlook, and others.
- Your Contacts:** Includes icons for Gmail, Facebook, Twitter, and others.
- Your Phone Calls:** Includes icons for a phone and Apple.
- Your Chat Conversations/ Messages:** Includes icons for Facebook, Twitter, and Amazon.
- Calendar Events:** Includes icons for a calendar and Facebook.
- Search History:** Includes icons for Google, Facebook, and others.
- Videos Watched:** Includes icons for YouTube, Twitter, and others.
- Websites Visited:** Includes icons for Google, Facebook, and others.
- Browser Information:** Includes icons for a laptop and Facebook.
- Video Uploads:** Includes icons for a camera and Facebook.
- Photo Uploads:** Includes icons for a camera and Facebook.
- About the Things Near Your Device (WiFi, Bluetooth, Etc.):** Includes icons for WiFi and Android.
- Voice Data:** Includes icons for a microphone and Android.
- Gaming Interactive Data:** Includes icons for a game controller and Xbox.
- Status Updates/Posts:** Includes icons for a pen and various social media logos.
- Likes:** Includes icons for a heart and various social media logos.
- Your Documents:** Includes icons for a document and Google Drive.
- Your Purchase History:** Includes icons for a shopping cart and Apple.
- Your Games:** Includes icons for a game controller and others.
- Your Books:** Includes icons for a book and others.
- Your Music:** Includes icons for a music note and others.
- Your Fitness/Health Data:** Includes icons for a person running and others.

Annotations provide additional context:

- Your Phone Calls:** Notes "Only the meta data on when the phone calls were made" and "Only the meta data on when the text messages ([in iMessage]) were made".
- Photo Uploads:** Notes "Including photo metadata".
- Status Updates/Posts:** Notes "Including discussion boards, community features, and reviews".
- Your Documents:** Notes "Only Apple device purchases and maintenance".
- Your Purchase History:** Notes "Only meta information on gaming sessions with Game Center".
- Your Music:** Notes "Including iTunes downloads as well as iTunes Match uploads and downloads".
- Your Fitness/Health Data:** Notes "HealthVault data such as heart rate and daily steps taken".
- Only Apple device:** Notes "Only Apple device".
- Includes skeletal tracking data and buttons pressed while using Xbox Live:** Notes "Includes skeletal tracking data and buttons pressed while using Xbox Live".

Sources:  
[www.privacy.google.com](http://www.privacy.google.com) | [www.policies.google.com](http://www.policies.google.com) |  
[www.facebook.com](http://www.facebook.com) | [www.newsroom.fb.com](http://www.newsroom.fb.com) |  
[www.washingtonpost.com](http://www.washingtonpost.com) | [www.apple.com](http://www.apple.com) | [www.zdnet.com](http://www.zdnet.com) |  
[www.twitter.com](http://www.twitter.com) | [www.fastcompany.com](http://www.fastcompany.com) | [www.amazon.com](http://www.amazon.com) |  
[www.androidcentral.com](http://www.androidcentral.com) | [www.privacy.microsoft.com](http://www.privacy.microsoft.com) |  
[www.wsj.com](http://www.wsj.com) | [www.ortune.com](http://www.ortune.com) | [www.fastcompany.com](http://www.fastcompany.com)

# 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 screenshot shows the homepage of CryptPad. At the top left is the logo "CryptPad" with a shield icon. At the top right are links for "Blog", "Pricing", "Privacy", and "xwikild". A teal banner at the top center states: "In the current health crisis linked to the COVID-19 outbreak, CryptPad supports remote working. The storage limit for all registered users is increased to 1GB until further notice. Registration is free with no personal data required." Below the banner, the CryptPad logo is displayed over a scenic mountain landscape. The text "The Zero Knowledge Cloud" is visible. To the right, there are icons for various features: "Rich text" (blue), "Code" (orange), "Presentation" (orange), "Sheet" (green), "Poll" (teal), "Kanban" (light green), "Whiteboard" (purple), and "CryptDrive" (blue). At the bottom left, a box contains text about the project being open-source and maintained by XWiki SAS. Another box explains the private-by-design nature of the service. A third box encourages support through a crowdfunding campaign, with a "Support CryptPad" button.

In the current health crisis linked to the COVID-19 outbreak, CryptPad supports remote working. The storage limit for all registered users is increased to 1GB until further notice. Registration is free with no personal data required.

**CryptPad**  
The Zero Knowledge Cloud

CryptPad.fr is the official instance of the open-source CryptPad project. It is administered by XWiki SAS, the employee-owned French company which created and maintains the product.

AGPL  
Free Software

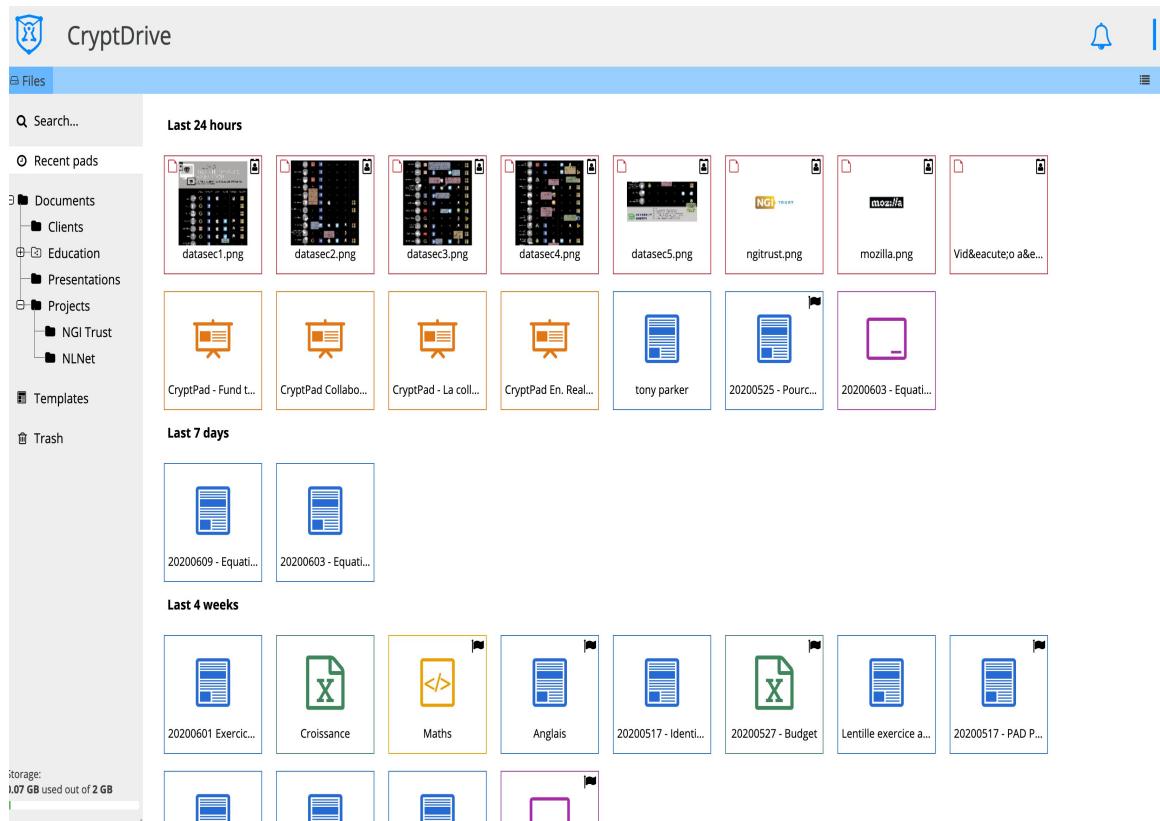
NGI AWARDS  
2019 winner

CryptPad is a private-by-design alternative to popular office tools and cloud services. All the content stored on CryptPad is encrypted before being sent, which means nobody can access your data unless you give them the keys (not even us).

CryptPad needs your help!  
Click on the button to learn about our crowdfunding campaign.

Support CryptPad

# CryptPad: Demo



# CryptPad: Demo

The screenshot shows the CryptPad web application interface. At the top, there's a navigation bar with 'File', 'Insert', 'Tools' (selected), 'Share', 'Access', and user status indicators ('Chat 2', '2 0'). Below the bar, a note titled 'What is CryptPad?' is displayed. The note content includes:

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

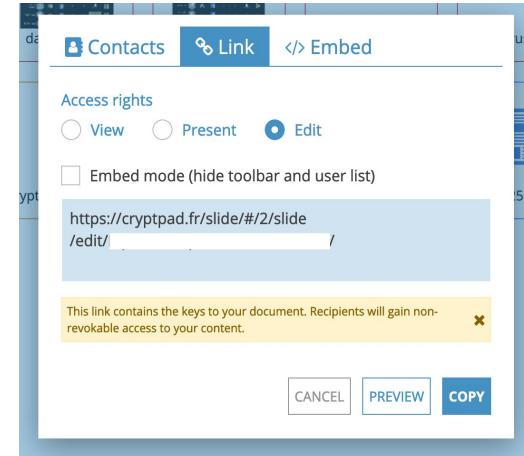
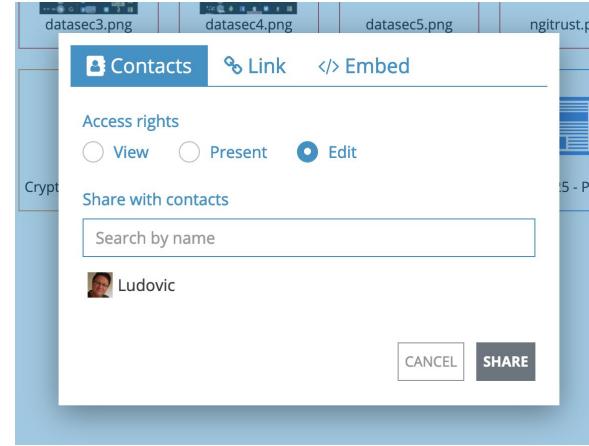
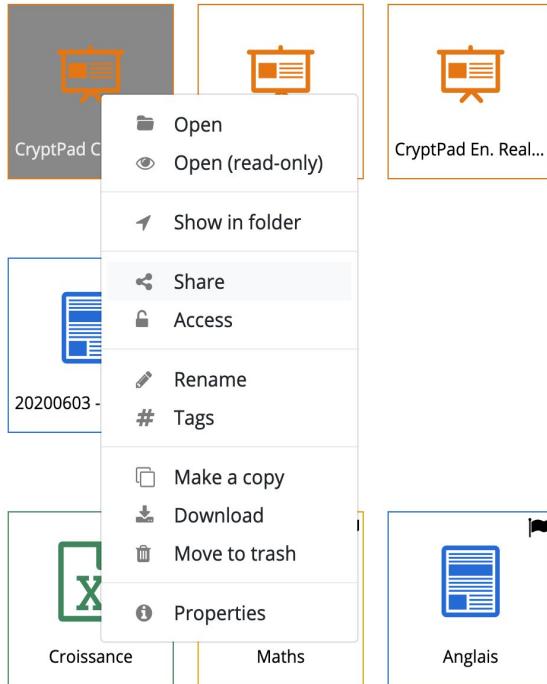
The right side of the interface shows a 'Users' panel with messages from 'ludotest' and 'Ludovic'. The messages are:

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

# CryptPad: Demo



# CryptPad: Demo

Mermaid mode test document Share Access Preview Chat 1 Users ludotest

File Theme Insert Tools

```
1 # Mermaid mode test document
2
3 [TOC]
4
5 ## Functional
6
7 /**
8 * -mermaid
9 generate
10 dateFormat: YYYY-MM-DD
11 title Adding GANTT diagram to mermaid
12
13
14 section A section
15 Completed task: done, des1, 2014-01-06,2014-01-08
16 Active task: active, des2, 2014-01-09, 3d
17 Future task: crit, done, des3, after des2, 5d
18 ..Future task2: des4, after des3, 5d
19
20
21 /**
22 */
23
24 /**
25 * -mermaid
26 pie title Pie Chart
27 :size
28   "Cats" : 85
29
30 Written by: ludotest
31
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 /**
54 graph TD
55
56 a
57 b((b))
58 c((c))
59 d((d))
60
61 f(((database)))
62 g((circle))
63 h((hexagon))
64 i((square))
65 j((hexagon))
66 k((parallelogram))
```

## Functional

### GANTT charts

Adding GANTT diagram to mermaid

The GANTT chart displays five tasks: 'Completed task' (grey bar), 'Active task' (blue bar), 'Future task' (red bar), 'Future task2' (dark blue bar), and 'A section' (light grey background). The x-axis represents dates from 01-07 to 01-21.

### Pie charts

Pie Chart

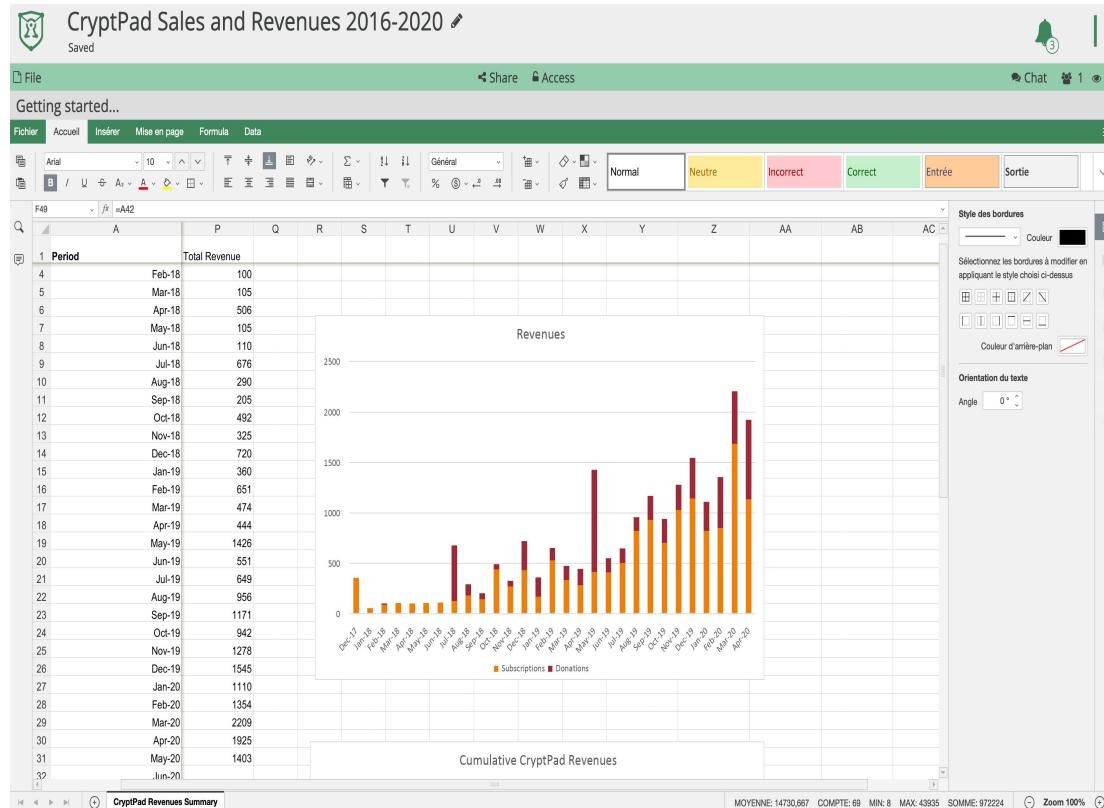
A pie chart divided into three segments: Dogs (62%), Cats (14%), and Rats (24%).

Category	Percentage
Dogs	62%
Cats	14%
Rats	24%

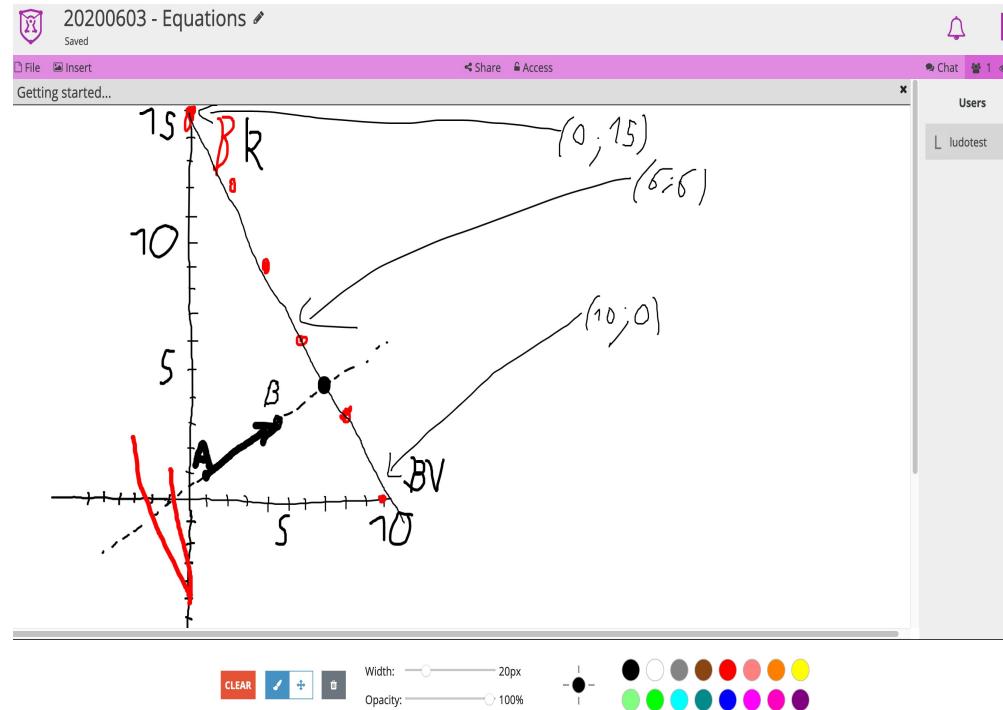
# CryptPad: Demo

Squad Kanban		File	Share	Access																
Saved																				
Filter by tag																				
accounts	admin august	communities1	communities3	communities4																
core	design documentation funding github infra july june kanban marketing moss october september server sheets smc smc1 smc2 smc3 smc4 smc5 support t	teams	website																	
<a href="#">Edit filter</a>																				
<div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> <p><b>Backlog/Ideas</b></p> <ul style="list-style-type: none"> <li>chainpad's onSettle is slow to call back <a href="#">core</a></li> <li>trim-history</li> <li><input checked="" type="checkbox"/> severes components <a href="#">CI tests</a></li> <li>server communities3</li> <li>use updated fast-diff in chainpad <a href="https://github.com/yichenfast-diff/react-11er4486123086679ee2c8f70e2fb44dfb2495">core</a></li> <li>write roster tests for INVITE and ACCEPT commands <a href="#">teams server</a></li> <li>Plan for how to remove things from the roster <a href="#">teams</a></li> <li>chainpad/istmp improvements <a href="#">core</a></li> <li><input checked="" type="checkbox"/> emit local changes as events in the chainpad and add a listener <a href="#">don't throw errors from chainpad, emit them with a handle</a></li> <li><input checked="" type="checkbox"/> consolidate chainpad - pending changes <a href="#">CT &amp; tests</a></li> <li><input checked="" type="checkbox"/> add authorship to chainpad <a href="#">october core</a></li> <li>open timeout while width, let the networking part of the worker handle that</li> <li>website - postgres update 9.6 to 11</li> </ul> </div> <div style="flex: 1;"> <p><b>Proposals</b></p> <ul style="list-style-type: none"> <li>the markdown "theme" dropdown loses its annotation after its first use <a href="#">Solved</a></li> </ul> </div> <div style="flex: 1;"> <p><b>Upcoming deadlines</b></p> <ul style="list-style-type: none"> <li>SMC1.1 protocol negotiation           <ul style="list-style-type: none"> <li>March 15th deadline <a href="#">Delayed by COVID19</a></li> <li>May 15th <a href="#">finish writing the SMC1.1 protocol negotiation spec</a></li> </ul> </li> <li>relative link <a href="#">smc server smc1 june</a></li> </ul> </div> <div style="flex: 1;"> <p><b>David</b></p> <ul style="list-style-type: none"> <li>Docs           <ul style="list-style-type: none"> <li>Sphinx repo</li> <li>French version from Yann Jaulin's draft</li> <li>Translate to english</li> <li>Set up translations</li> </ul> </li> <li>community3 design <a href="#">u</a></li> </ul> </div> <div style="flex: 1;"> <p><b>Aaron</b></p> <ul style="list-style-type: none"> <li>metadata queries for empty files return E_NO OWNERS instead of ENDENT <a href="#">see here</a></li> <li>What does this break? <a href="#">What happens if I remove a pad from the server in the drive. If the pad is already deleted, it tells me it can't own an owner. The server should tell me it doesn't exist so that I can remove the pad from the drive</a></li> <li>server</li> </ul> </div> <div style="flex: 1;"> <p><b>Yann</b></p> <ul style="list-style-type: none"> <li>prepare accounts next steps <a href="#">accounts</a></li> <li>read only spreadsheets are blank</li> <li>• tickets           <ul style="list-style-type: none"> <li>relevant support ticket</li> <li>another</li> <li>relevant issue</li> </ul> </li> <li>the correct content is displayed when the pad is first loaded, but it does not update with any new edits made after load time</li> <li>• prevent the file from being the editor request looks (but in UO)           <ul style="list-style-type: none"> <li>1. the file gives edit option</li> <li>If you insist, you are able to force the lock sometimes (I don't know why)</li> <li>then you need to make a node in cryptdrive where you don't use the locks but your content is not pushed in realtime, you have to press a "Save" button and then you will be able to enable it with write protection</li> <li>haven't found yet</li> <li>warn viewers and editors that share view links that view mode doesn't update in real time</li> <li>display warning that the document is out of date when remote patches arrive... click to display the latest edits, shortly displaying this so that you're not constantly warned</li> </ul> </li> <li>sheets <a href="#">github</a> <a href="#">u</a></li> </ul> </div> <div style="flex: 1;"> <p><b>Needs review</b></p> <ul style="list-style-type: none"> <li>master/main branches <a href="#">toons are drafted in this pad</a></li> <li>admin marketing <a href="#">Yann</a></li> <li>U release <a href="#">plan feature set</a></li> <li>notes</li> </ul> </div> <tr> <td colspan="5"> <div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> <p>disable "empty trash" if the trash is empty <a href="#">sweet branch</a></p> </div> <div style="flex: 1;"> <p>remove extra text from the tag prompt <a href="#">prompt</a></p> </div> </div> </td></tr> <tr> <td colspan="5"> <p>"Start a search with # in your CryptDrive to find your tagged pads."</p> <p>Modifying the code to do what you want is not trivial. <a href="#">CryptDrive</a> <a href="#">GitHub</a></p> <p>The most recent change was made on <a href="#">2021-03-11</a> at <a href="#">10:45 UTC</a>.</p> </td></tr> <tr> <td colspan="5"> <p><b>Improve the support/admin panels</b></p> <ul style="list-style-type: none"> <li>suggested categories for tickets</li> <li>a method of filtering those tickets for admins</li> <li>pad interface with clear warnings about:           <ul style="list-style-type: none"> <li>to be able to provide access to a corrupted pad, for instance</li> <li>(im)format to markdown is probably too geeky</li> <li>attachments</li> <li>for screenshots, etc.</li> </ul> </li> <li>support</li> </ul> </td></tr> <tr> <td colspan="5"> <p>drive github issues</p> </td></tr> </div>	<div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> <p>disable "empty trash" if the trash is empty <a href="#">sweet branch</a></p> </div> <div style="flex: 1;"> <p>remove extra text from the tag prompt <a href="#">prompt</a></p> </div> </div>					<p>"Start a search with # in your CryptDrive to find your tagged pads."</p> <p>Modifying the code to do what you want is not trivial. <a href="#">CryptDrive</a> <a href="#">GitHub</a></p> <p>The most recent change was made on <a href="#">2021-03-11</a> at <a href="#">10:45 UTC</a>.</p>					<p><b>Improve the support/admin panels</b></p> <ul style="list-style-type: none"> <li>suggested categories for tickets</li> <li>a method of filtering those tickets for admins</li> <li>pad interface with clear warnings about:           <ul style="list-style-type: none"> <li>to be able to provide access to a corrupted pad, for instance</li> <li>(im)format to markdown is probably too geeky</li> <li>attachments</li> <li>for screenshots, etc.</li> </ul> </li> <li>support</li> </ul>					<p>drive github issues</p>				
<div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> <p>disable "empty trash" if the trash is empty <a href="#">sweet branch</a></p> </div> <div style="flex: 1;"> <p>remove extra text from the tag prompt <a href="#">prompt</a></p> </div> </div>																				
<p>"Start a search with # in your CryptDrive to find your tagged pads."</p> <p>Modifying the code to do what you want is not trivial. <a href="#">CryptDrive</a> <a href="#">GitHub</a></p> <p>The most recent change was made on <a href="#">2021-03-11</a> at <a href="#">10:45 UTC</a>.</p>																				
<p><b>Improve the support/admin panels</b></p> <ul style="list-style-type: none"> <li>suggested categories for tickets</li> <li>a method of filtering those tickets for admins</li> <li>pad interface with clear warnings about:           <ul style="list-style-type: none"> <li>to be able to provide access to a corrupted pad, for instance</li> <li>(im)format to markdown is probably too geeky</li> <li>attachments</li> <li>for screenshots, etc.</li> </ul> </li> <li>support</li> </ul>																				
<p>drive github issues</p>																				

# 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

50000+ users  
per week

350000+ pads  
open per  
week

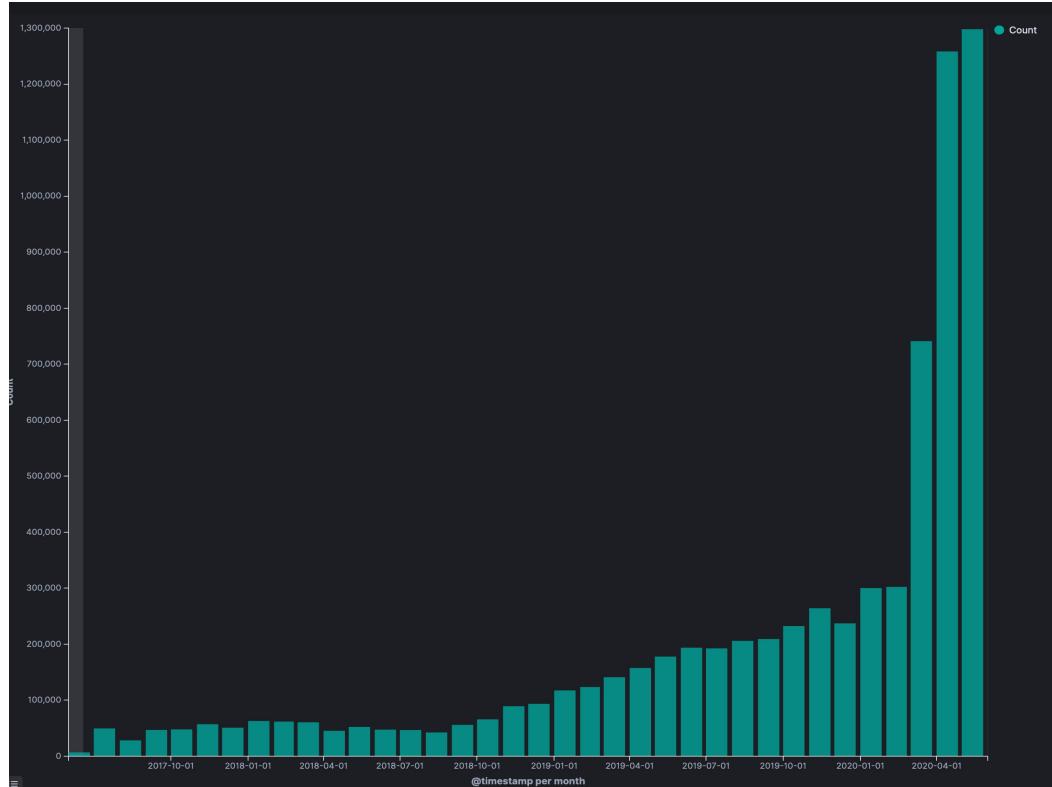


450 installs

Heavy usage in Germany

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)

20K Euros for 2020

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