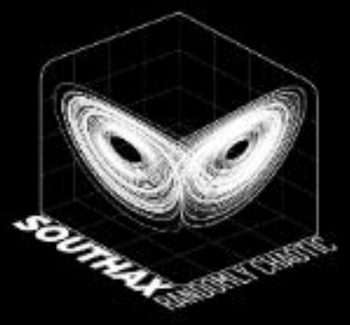
dor1an2FA:

making authentication easier with a twist

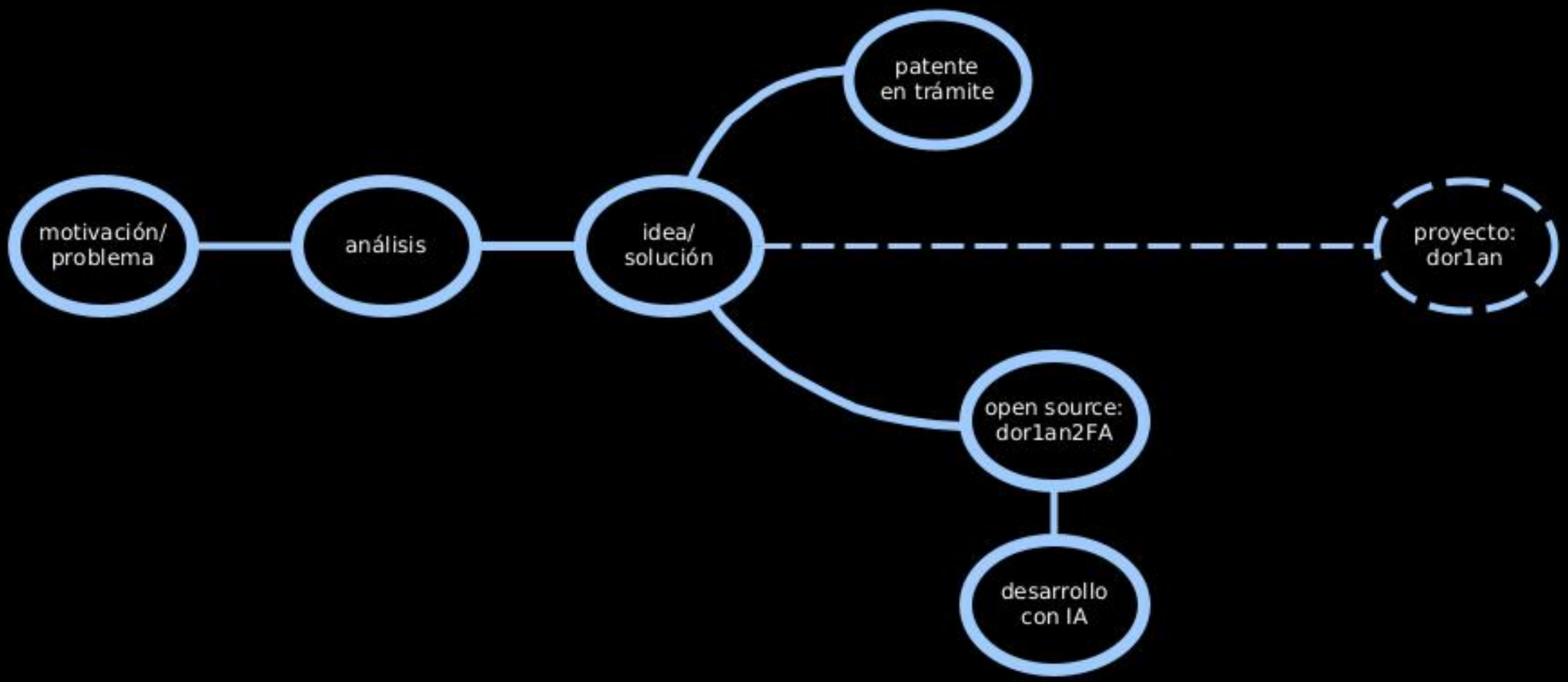


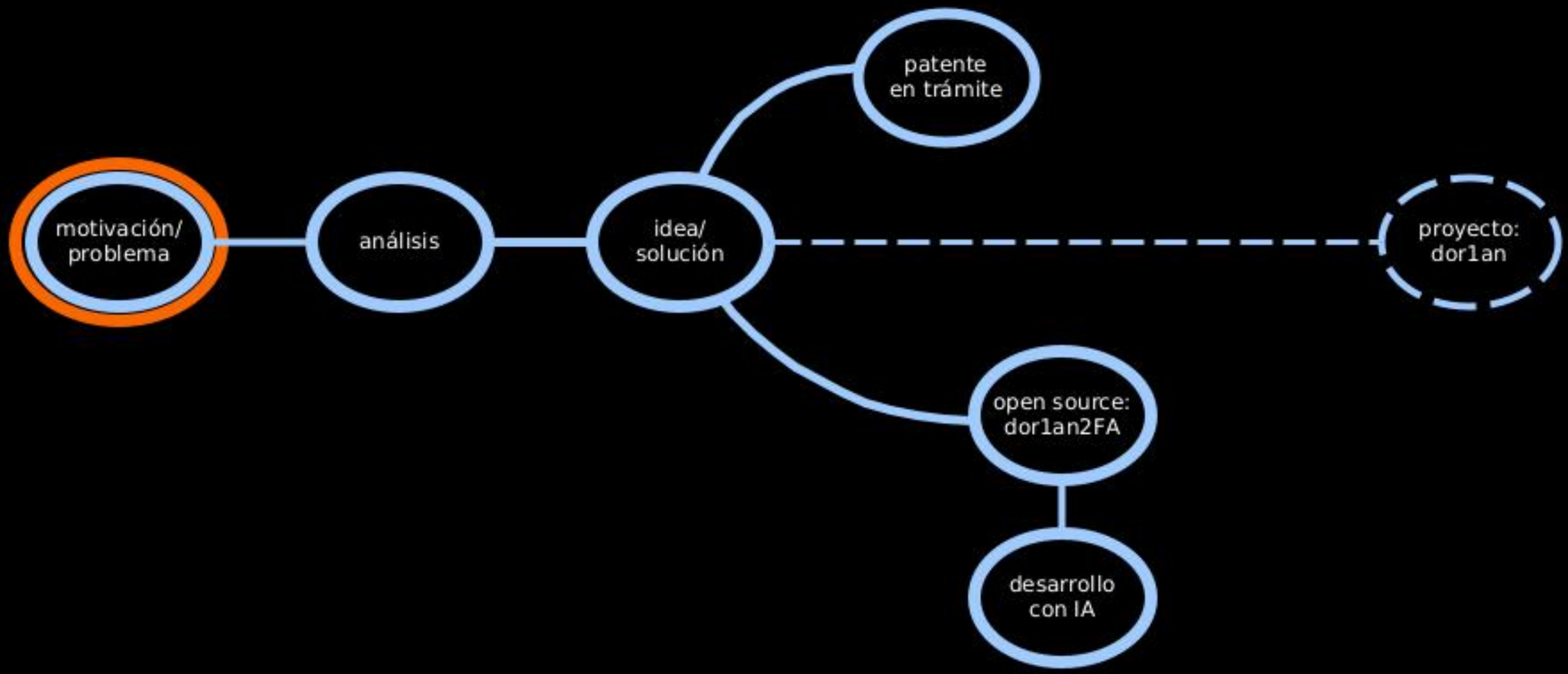
Ekoparty #20
13 de Noviembre de 2024
Carlos Benitez

Carlos Benitez

- Ing. y Mg. de la UTN FRBA
- Investigador en procesamiento de señales acústicas submarinas.
- Director del primer Laboratorio en Seguridad Informática (Si6) en el ámbito del Estado.
- Implementación del primer SOC del Ministerio de Defensa.
- Asesor técnico de la Subsecretaría de Ciberdefensa.
- Consultor en ciberseguridad.
- Co-fundador de Platinumciber.
- Proyectos de ciberseguridad, como: SOC, Ethical Hacking, Vulnerability Assessment, Análisis forense, Análisis y Gestión de Riesgos, etc.
- Algunas publicaciones en congresos y dos patentes en USA en ciberseguridad.
- Docente de posgrado en ciberseguridad.
- Formador y mentoring de teams.
- Quantum Computing enthusiast.

Índice


patente
en trámite
motivación/
problema
análisis
idea/
solución
proyecto:
dor1an
open source:
dor1an2FA
desarrollo
con IA

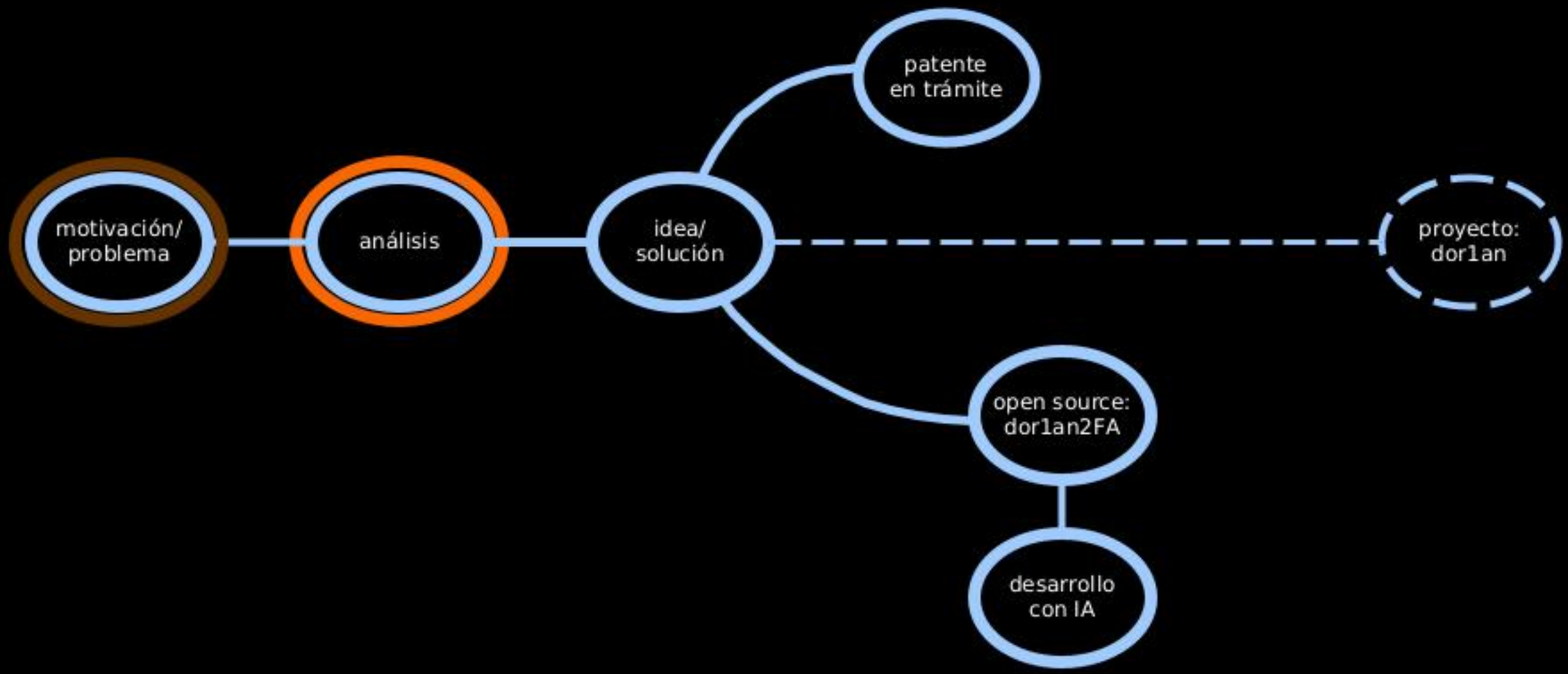

motivación/
problema
análisis
idea/
solución
patente
en trámite
proyecto:
dor1an
open source:
dor1an2FA
desarrollo
con IA

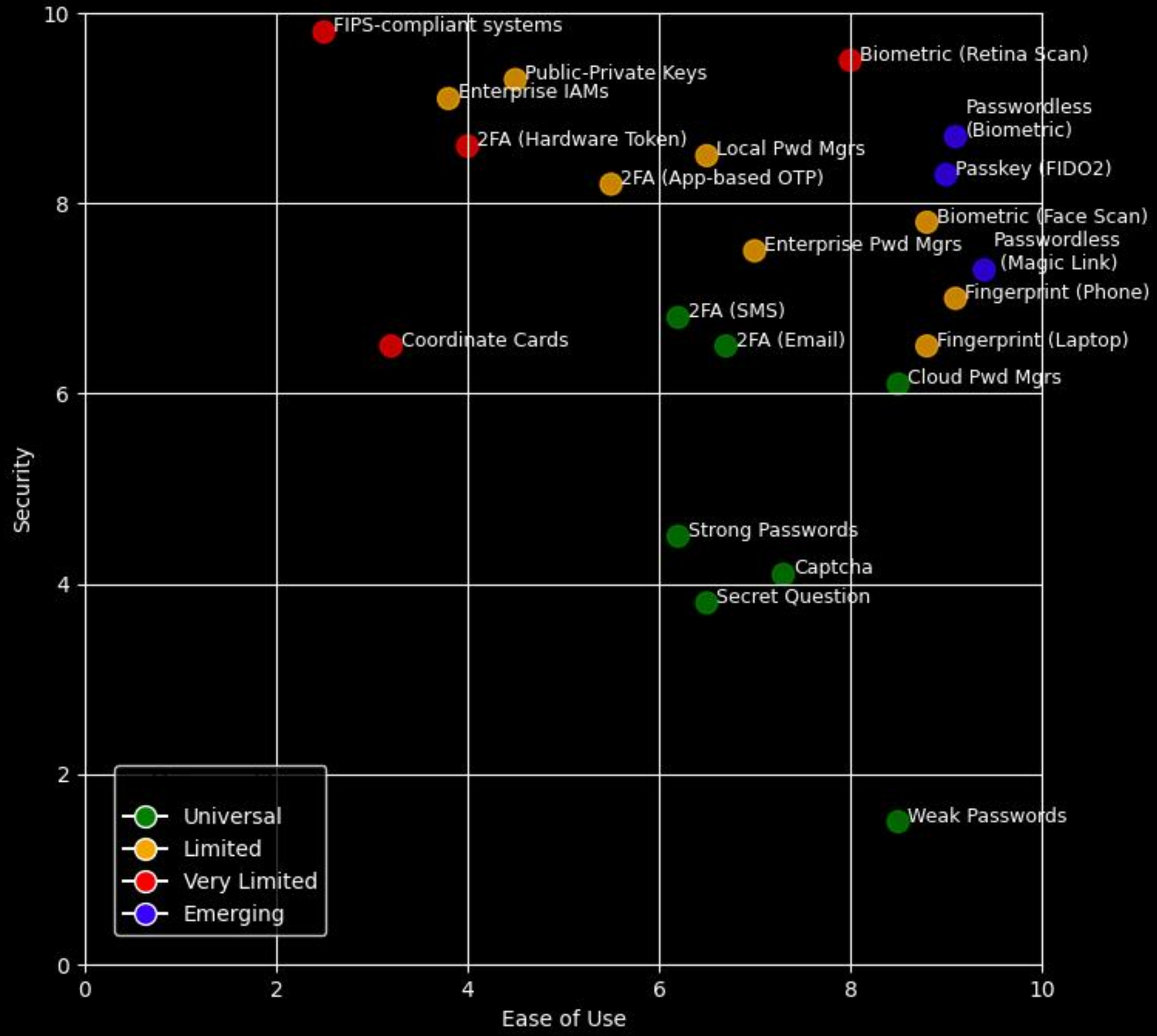

ALGUIEN QUIERE PENSAR EN LOS USUARIOS!
imgflip.com

todos somos capa 8...

todos hemos estado alguna vez, en modo capa 8...

Cómo hago para seguir seguro
pero no escribir más contraseñas?

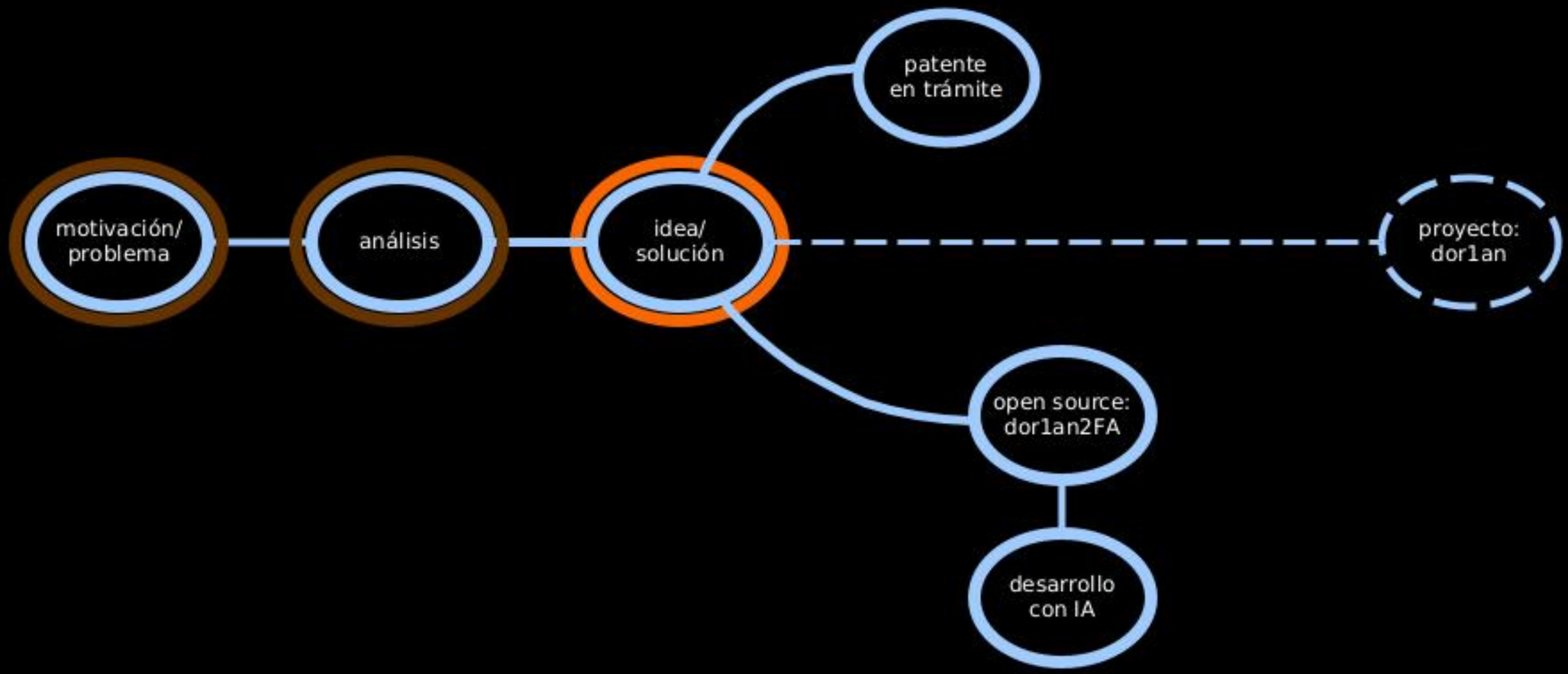

motivación/
problema
análisis
idea/
solución
patente
en trámite
proyecto:
dor1an
open source:
dor1an2FA
desarrollo
con IA



Authentication Methods: Ease of Use vs Security

password managers:

ONE PASSWORD TO RULE THEM ALL


patente
en trámite
motivación/
problema
análisis
idea/
solución
proyecto:
dor1an
open source:
dor1an2FA
desarrollo
con IA

facilidad de uso:
comunicación bidireccional
cámara-pantalla

seguridad:
SSS (Shamir Secret Sharing)

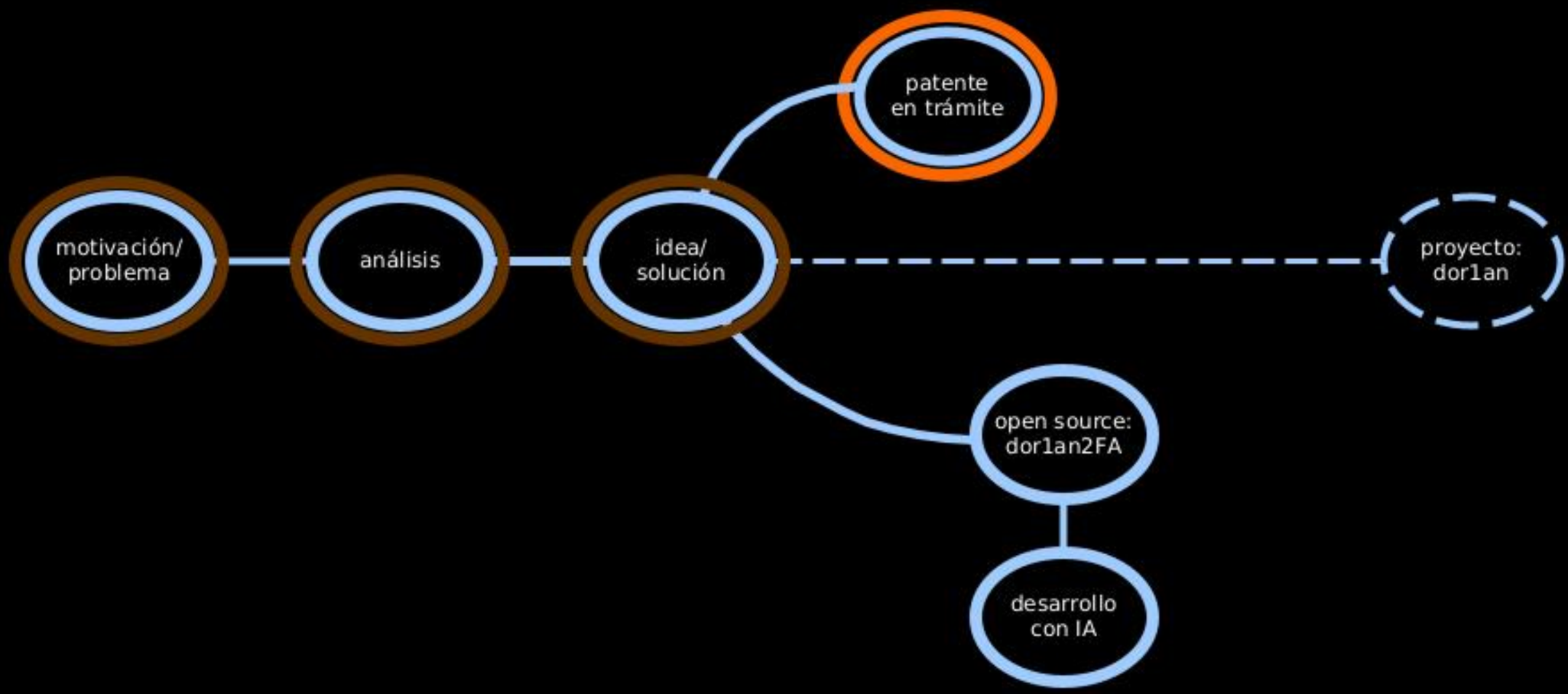
```
(base) test@darp10:~$ #Password is: ABCDEFGHIJK
(base) test@darp10:~$ ssss-split -t 3 -n 10
Generating shares using a (3,10) scheme with dynamic security level.
Enter the secret, at most 128 ASCII characters: Using a 88 bit security level.
01-da872dbee3be8275cdee2a
02-a2007b3b9916045bef4d1f
03-9be29104a7b8e594ca17e5
04-ab2f1de5b0723d85d277f8
05-92cdf7da8edcdc4af72d10
06-ea4aa15ff4745a64d58e01
07-d3a84b60cadabbabf0d4ef
08-59f6ff0a926e983049f2f5
09-60141535acc079ff6ca841
10-189343b0d668ffd14e0b9c
(base) test@darp10:~$ ssss-combine -t 3
Enter 3 shares separated by newlines:
Share [1/3]: 03-9be29104a7b8e594ca17e5
Share [2/3]: 06-ea4aa15ff4745a64d58e01
Share [3/3]: 10-189343b0d668ffd14e0b9c
Resulting secret: ABCDEFGHIJK
(base) test@darp10:~$
```

seguridad:
SSS (Shamir Secret Sharing)

```
(base) test@darp10:~$ apt changelog ssss|grep -A4 Initial

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

  * Initial release.

 -- David Moreno Garza <damog@debian.org>  Sun, 23 Oct 2005 16:22:30 -0500
Fetched 2,373 B in 1s (1,858 B/s)
(base) test@darp10:~$
```

seguridad:

2FA(TOTP) = N/A


patente
en trámite
motivación/
problema
análisis
idea/
solución
proyecto:
dor1an
open source:
dor1an2FA
desarrollo
con IA

Applying for a patent

Design patent guide

Plant patent guide

Utility patent guide

Provisional applications

File Online

File a patent application online with Patent Center

Maintenance Fees

Estimate your patent maintenance fees

Contact Us
Local: 1-800-786-9199

Provisional Application for Patent

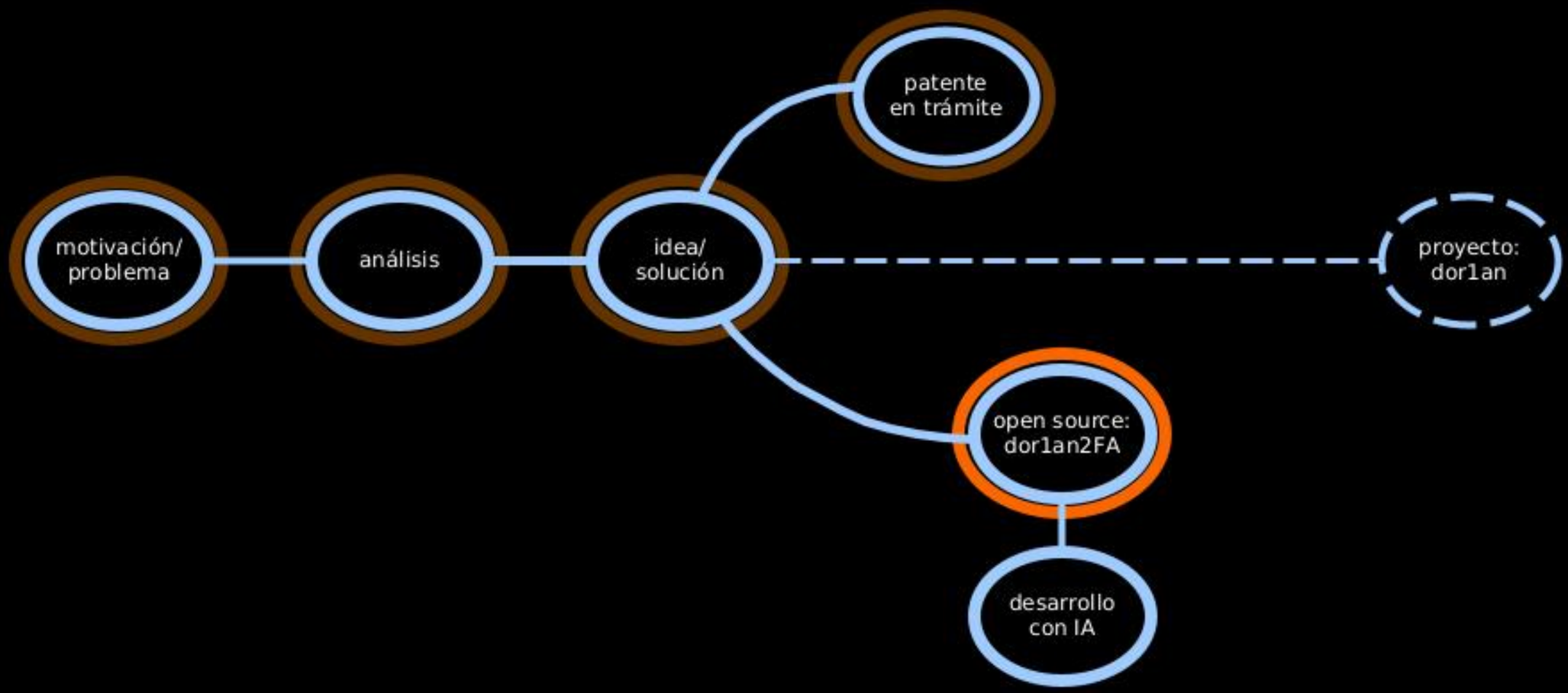
Provisional patent application forms

A provisional patent application allows you to file without a formal patent claim, oath or declaration, or any information disclosure (prior art) statement.

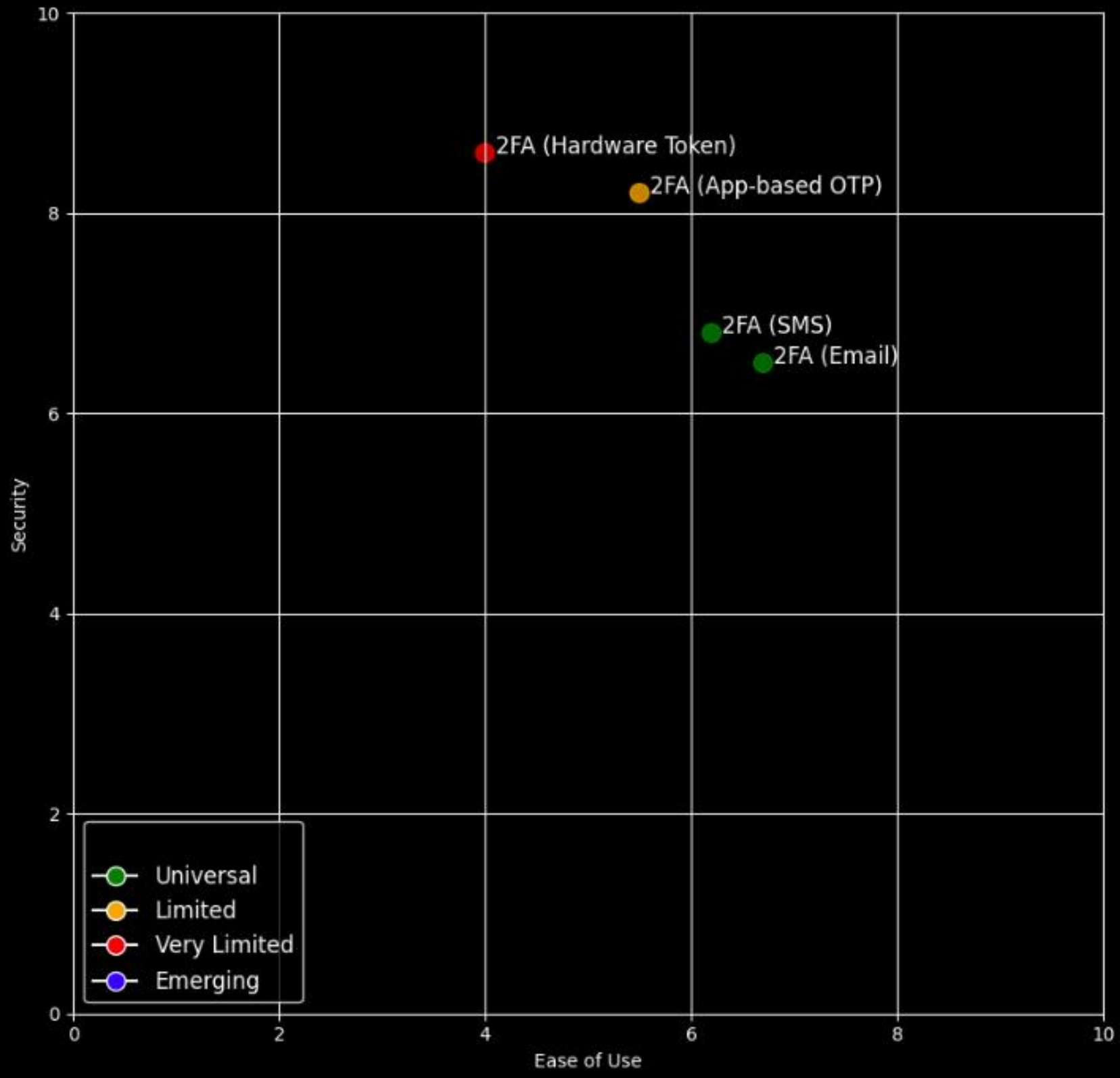
Since June 8, 1995, the United States Patent and Trademark Office (USPTO) has offered inventors the option of filing a provisional application for patent which was designed to provide a lower-cost first patent filing in the United States and to give U.S. applicants parity with foreign applicants under the GATT Uruguay Round Agreements.

A provisional application for patent (provisional application) is a U.S. national application filed in the USPTO under 35 U.S.C. §111(b). A provisional application is not required to have a formal patent claim or an oath or declaration. Provisional applications also should not include any information disclosure (prior art) statement since provisional applications are not examined. A provisional application provides the means to establish an early effective filing date in a later filed nonprovisional patent application filed under 35 U.S.C. §111(a). It also allows the term "Patent Pending" to be applied in connection with the description of the invention.

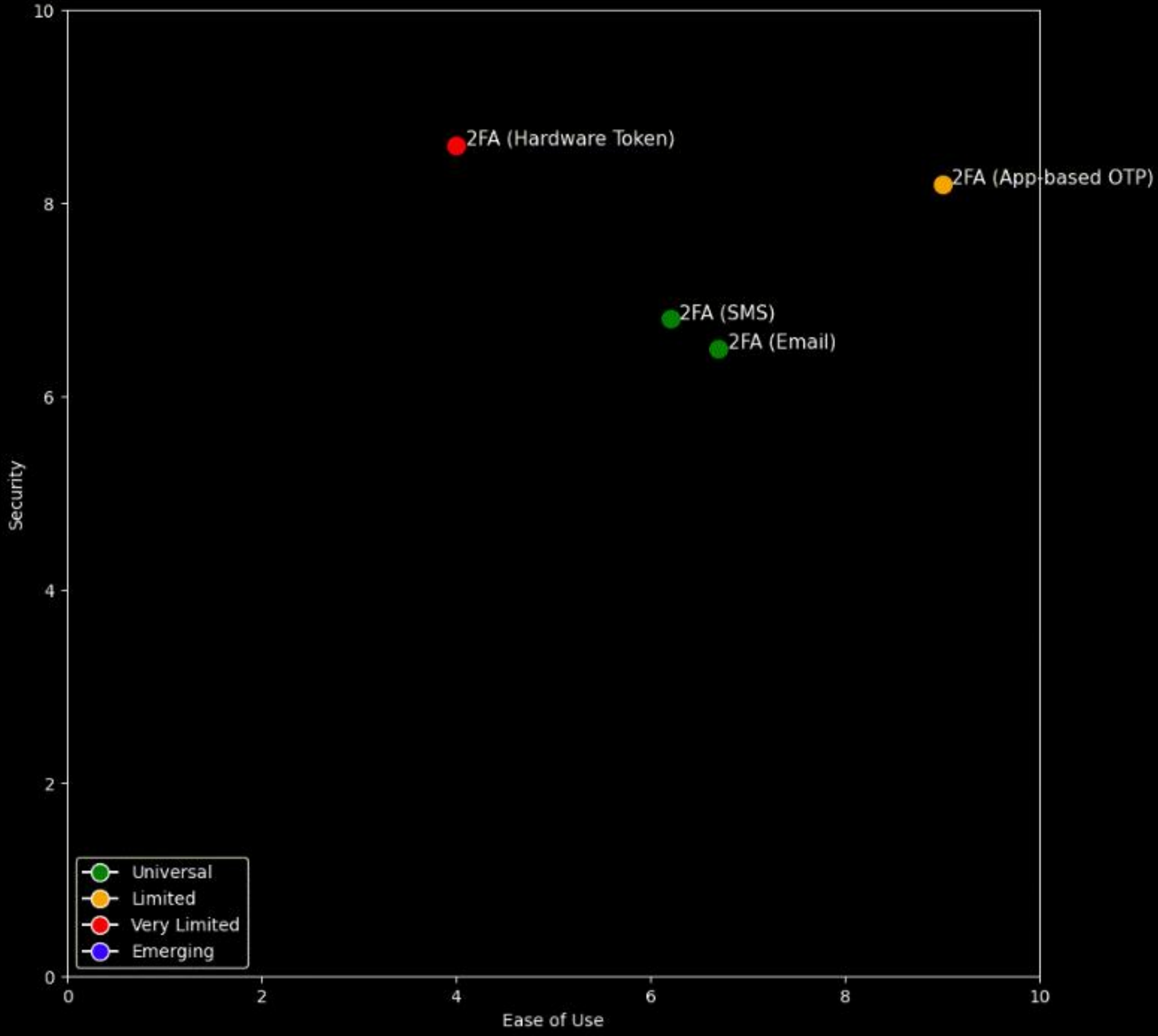
A provisional application for patent has a pendency lasting 12 months from the date the provisional application is filed. **The 12-month pendency period cannot be extended.** Therefore, an applicant who files a provisional application must file a corresponding nonprovisional application for patent (nonprovisional application) during the 12-month pendency period of the provisional application in order to benefit from the earlier filing of the provisional application. However, a nonprovisional application that was filed more than 12 months after the filing date of the provisional application, but within 14 months after the filing date of the provisional application, may have the benefit of the provisional application restored by filing a grantable petition (including a statement that the delay in filing the nonprovisional application was unintentional and the required petition fee) to restore the benefit under 37 CFR 1.78.


patente
en trámite
motivación/
problema
análisis
idea/
solución
proyecto:
dor1an
open source:
dor1an2FA
desarrollo
con IA

el problema más sencillo:
el segundo factor



2FA Authentication Methods: Ease of Use vs Security (Detailed)


2FA (Hardware Token)
2FA (App-based OTP)
2FA (SMS)
2FA (Email)
Universal
Limited
Very Limited
Emerging
Security
Ease of Use
0
2
4
6
8
10

La app I: dor1an2FA

La app I: dor1an2FA

USPTO Patent pending

dor1an2FA

USPTO Patent pending

una demo vale más que mil palabras

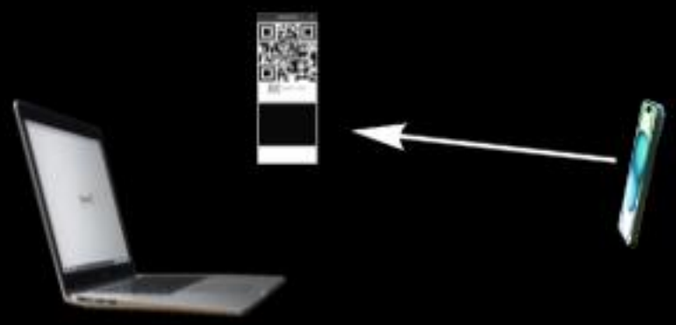
demo time!

flujo

#1: la extensión detecta que se debe ingresar el 2F

#2: la extensión crea un QR con el hostname y prende la cámara

#3: el usuario levanta la app y enfrenta el celular a la pantalla de la laptop.

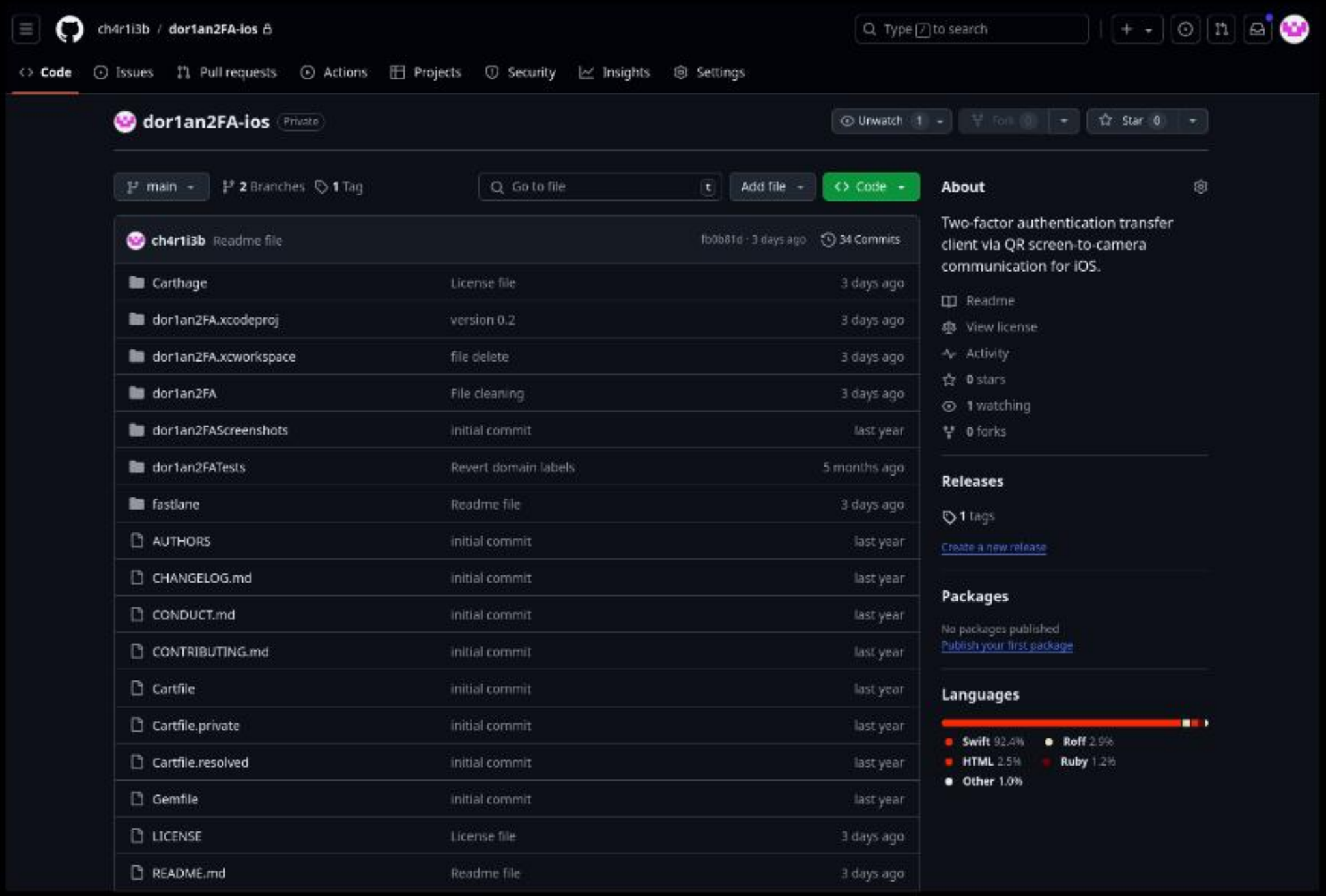


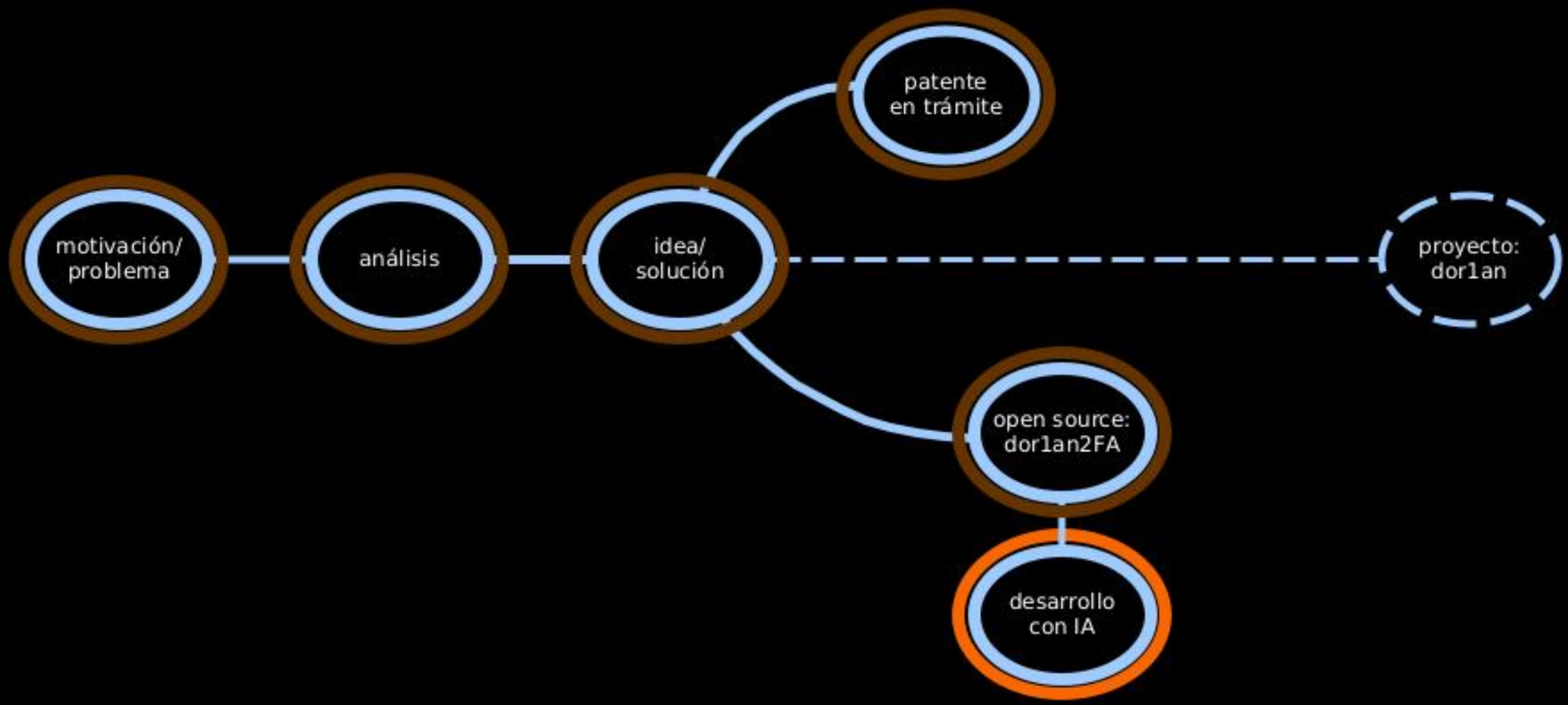
#4: la app lee el QR, si el hostname es válido, crea el QR con el TOTP

#5: la extension lee el QR, con el TOTP, lo decodifica y lo pasa a la textbox

#6: login exitoso

github


ch4r1i3b / dor1an2FA-ios
Type / to search
Code
Issues
Pull requests
Actions
Projects
Security
Insights
Settings
dor1an2FA-ios
Private
Unwatch 1
Fork 0
Star 0
main
2 Branches
1 Tag
Go to file
t
Add file
Code
ch4r1i3b Readme file
fb0b81d · 3 days ago
34 Commits
Carthage License file 3 days ago
dor1an2FA.xcodeproj version 0.2 3 days ago
dor1an2FA.xcworkspace file delete 3 days ago
dor1an2FA File cleaning 3 days ago
dor1an2FAScreenshots initial commit last year
dor1an2FATests Revert domain labels 5 months ago
fastlane Readme file 3 days ago
AUTHORS initial commit last year
CHANGELOG.md initial commit last year
CONDUCT.md initial commit last year
CONTRIBUTING.md initial commit last year
Cartfile initial commit last year
Cartfile.private initial commit last year
Cartfile.resolved initial commit last year
Gemfile initial commit last year
LICENSE License file 3 days ago
README.md Readme file 3 days ago
About
Two-factor authentication transfer client via QR screen-to-camera communication for iOS.
Readme
View license
Activity
0 stars
1 watching
0 forks
Releases
1 tags
Create a new release
Packages
No packages published
Publish your first package
Languages
Swift 92.4%
Roff 2.9%
HTML 2.5%
Ruby 1.2%
Other 1.0%


patente
en trámite
motivación/
problema
análisis
idea/
solución
proyecto:
dor1an
open source:
dor1an2FA
desarrollo
con IA

desarrollo con AI

Authenticator (Matt Rubin)

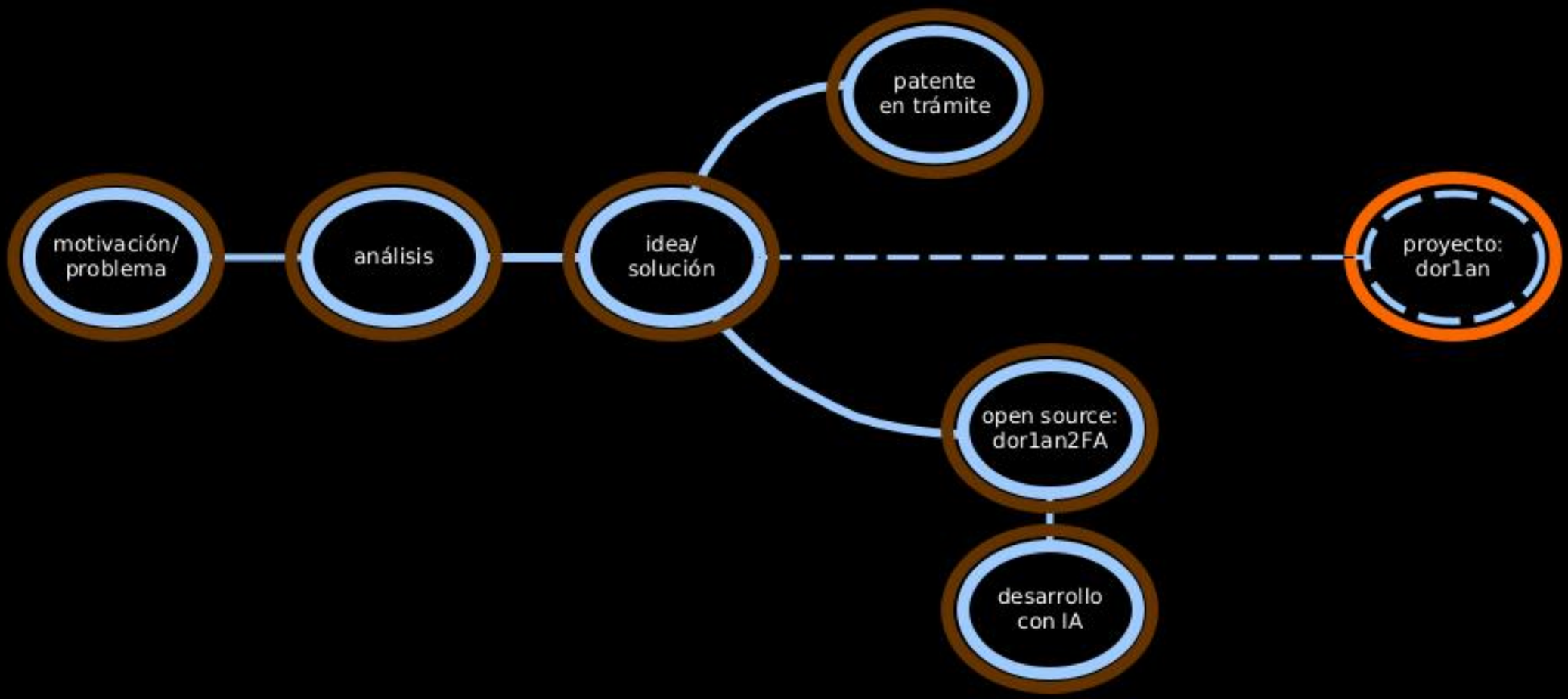
https://github.com/mattrubin/Authenticator

desarrollo con AI

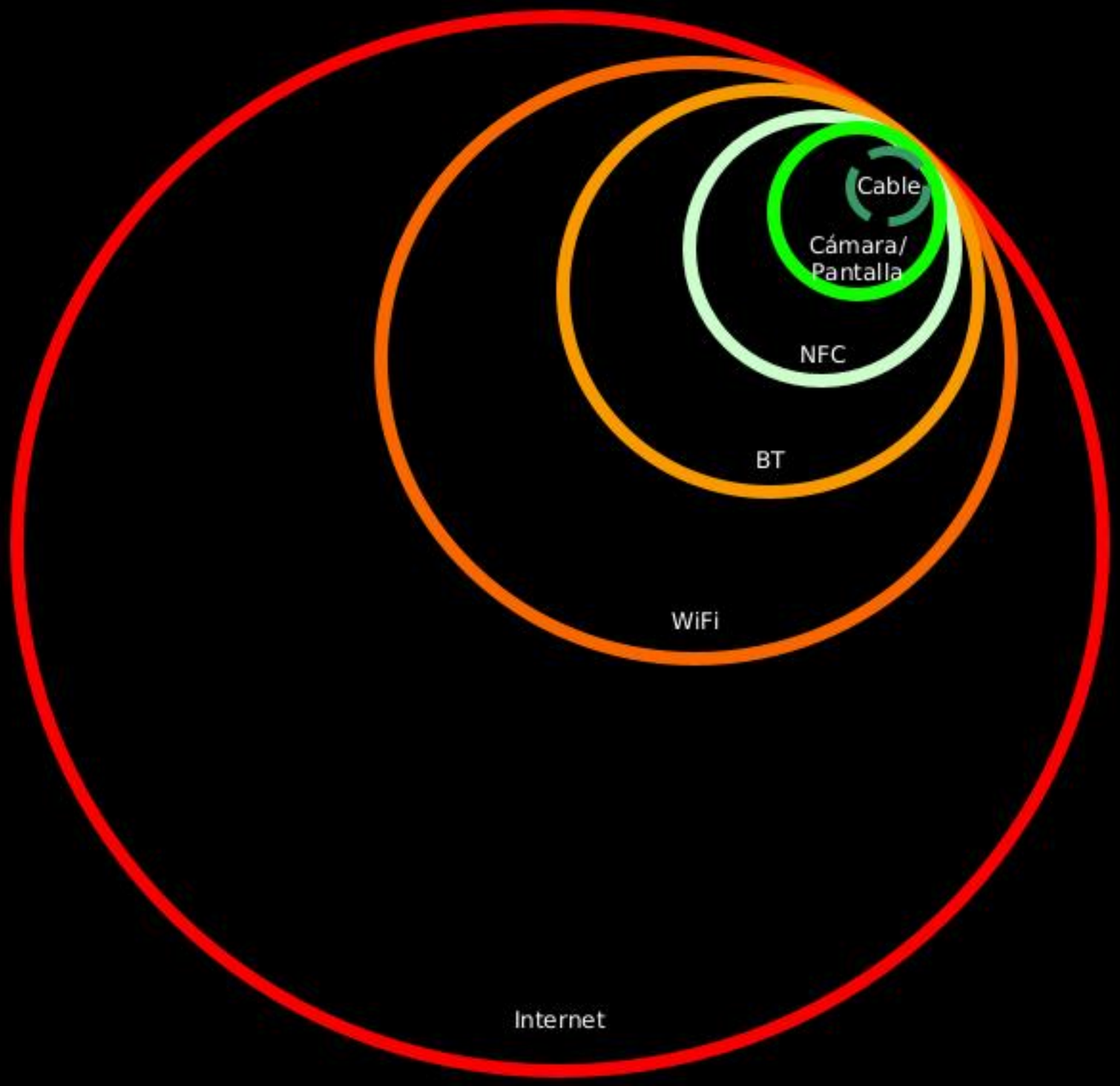
- ChatGPT
- Git copilot
- Askcodi
- ChatGPT Swift

desarrollo con AI

- las 10 preguntas
- curva ideal vs. curva real
- no sirve pelearse

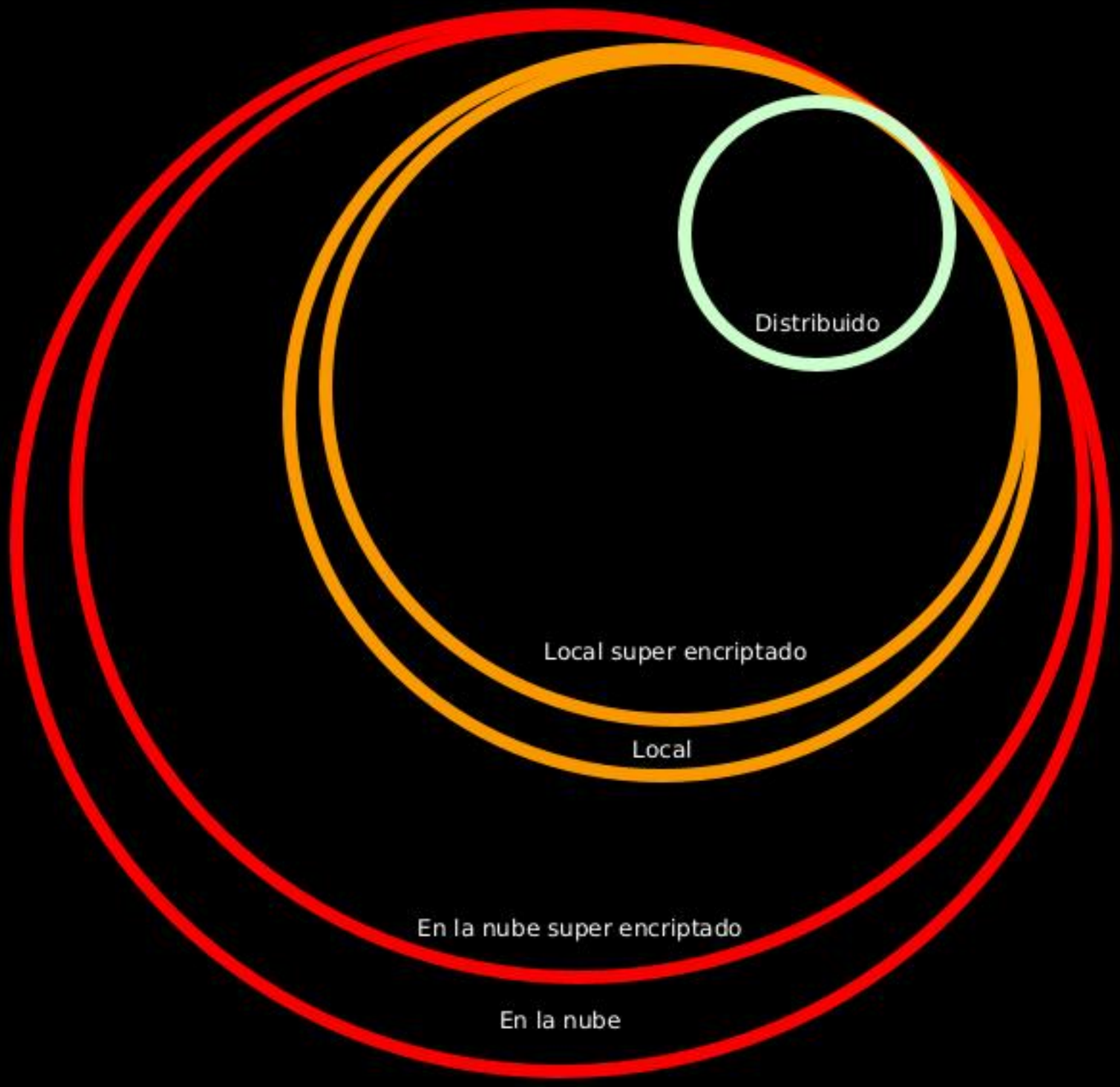

patente
en trámite
motivación/
problema
análisis
idea/
solución
proyecto:
dor1an
open source:
dor1an2FA
desarrollo
con IA

método de transmisión



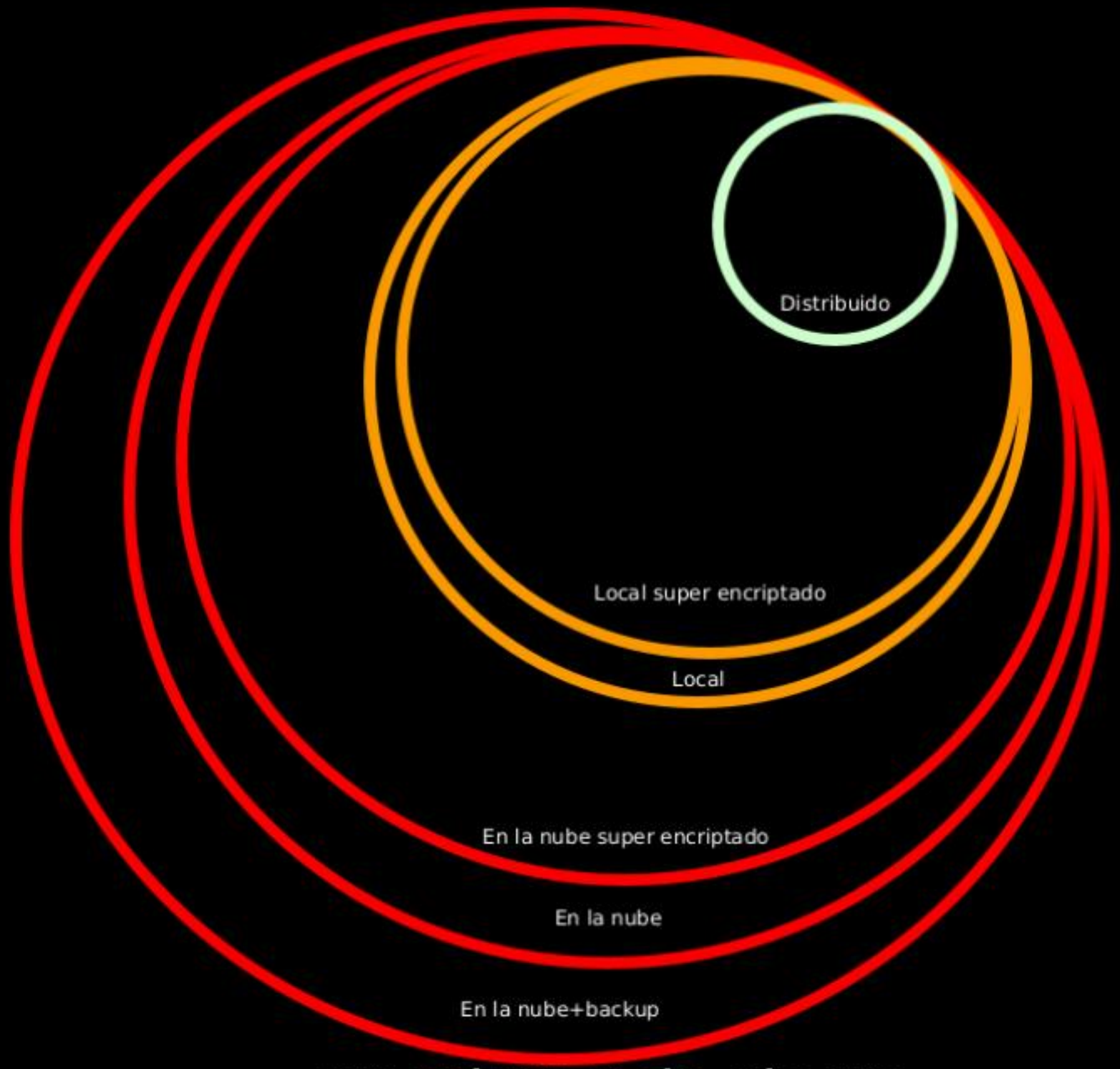
superficies de ataque

almacenamiento de secretos



superficies de ataque

almacenamiento de secretos



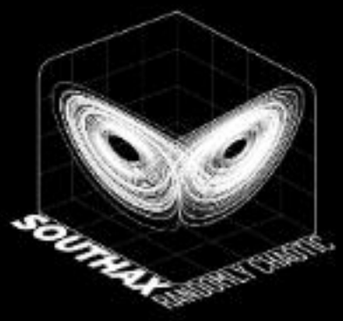
superficies de ataque

Conclusiones

- método para transferir secretos via cámara/pantalla
- método para almacenar secretos vía password split (sss)
- desarrollo open source: dor1an2FA
- proyecto completo: dor1an
- usen, rompan y critiquen.

GRACIAS!!!!

A la Eko
A Kennbro (Southax)
A Matt Rubin



Carlos Benitez
@ch4r1i3b
carlos<at>platinumciber.com
https://cybersonthestorm.com
https://github.com/ch4r1i3b

Ekoparty #20
13 de Noviembre de 2024
Carlos Benitez