IDENTITÉ DÉCENTRALISÉE

MYTHE OU RÉALITÉ

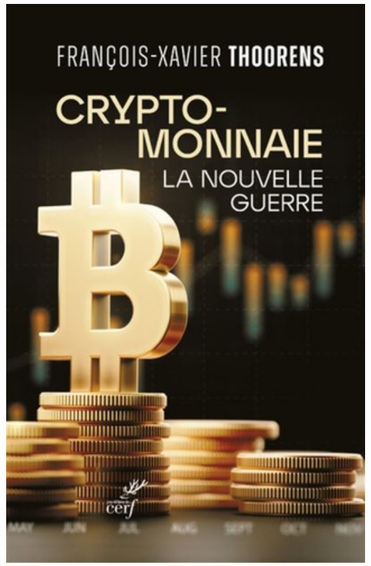
14/01/2025 Réunion OSSIR, Campus Cyber

FRANÇOIS-XAVIER THOORENS

Scientific Officer - EU JRC / BSCPS

Developper and CEO of ark.io

Currently CEO of Vaultys



PROGRAMME

01 Historique

02 Bitcoin

03 Approche Vaultys

04 Problèmes

05 Identity vs KYC

01

HISTORIQUE

Signing party!

HISTORIQUE

1977 : **RSA**
1988 : **X.509 / PKI**
1991 : Phil Zimmerman, invention de **PGP** RFC 4880
1992 : Concept de **Web of Trust**
1995 : **SSL** (Netscape)
1999 : **TLS**
2005 : Zimmermann-Sassaman **key-signing protocol**
2009 : **Bitcoin, WhatsApp**
2014 : **FIDO U2F / Yubikey**
2015 : **Rebooting the Web of Trust** (papers)
2016 : Christopher Allen, **The Path to Self-Sovereign Identity**
2019 : W3C **Verifiable Credentials**, **WebAuthn**
2022 : W3C **DIDs** v1.0, Vaultys

Phil Zimmermann

WEB OF TRUST (WOT)

As time goes on, **you will accumulate keys from other people** that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers.

And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the **emergence of a decentralized fault-tolerant web of confidence for all public keys.**

QUI UTILISE CES TECHNOLOGIES ?

- Signing party ?
- PGP certificate pour signer / chiffrer les emails ?
- Déploiement d’un serveur HKS ?
- keys.openpgp.org ?
- DiD ? VC ?
- Hardware key ?
- Multisignature ?

2015

Sorry, but I cannot decrypt this message. I don't have a version of PGP that runs on any of my devices

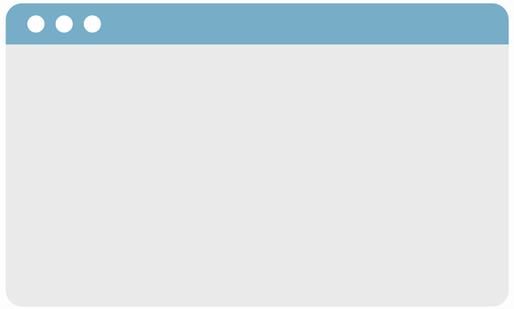
2015

Sorry, but I cannot decrypt this message. I don't have a version of PGP that runs on any of my devices

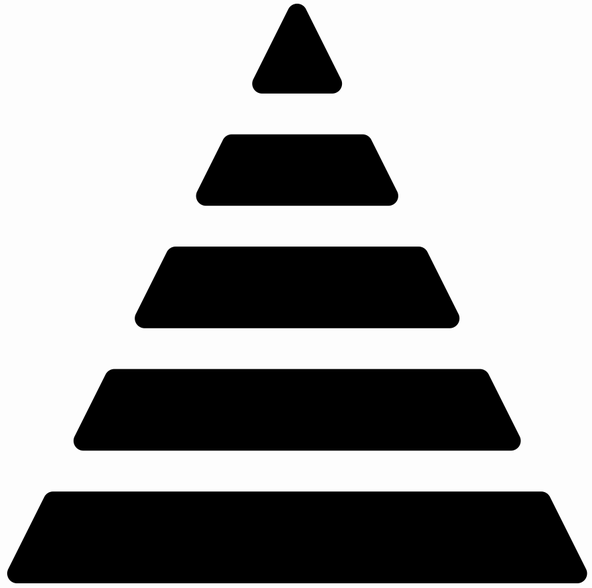
ALTERNATIVES

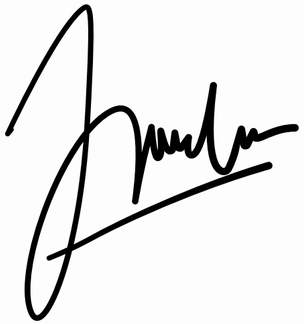
- PGP Efail -> WhatsApp, Signal, Olvid, DeltaChat (PGP+Email)
- File encryption -> Age, many others
- Web of Trust -> Blockchain ?
- Signing Party -> ?
- Key Manager -> Webauthn, youbikeys, Ledger, MetaMask, WalletConnect

INTERNET SECURITY



let’s encrypt





check your mail

PKI

ET

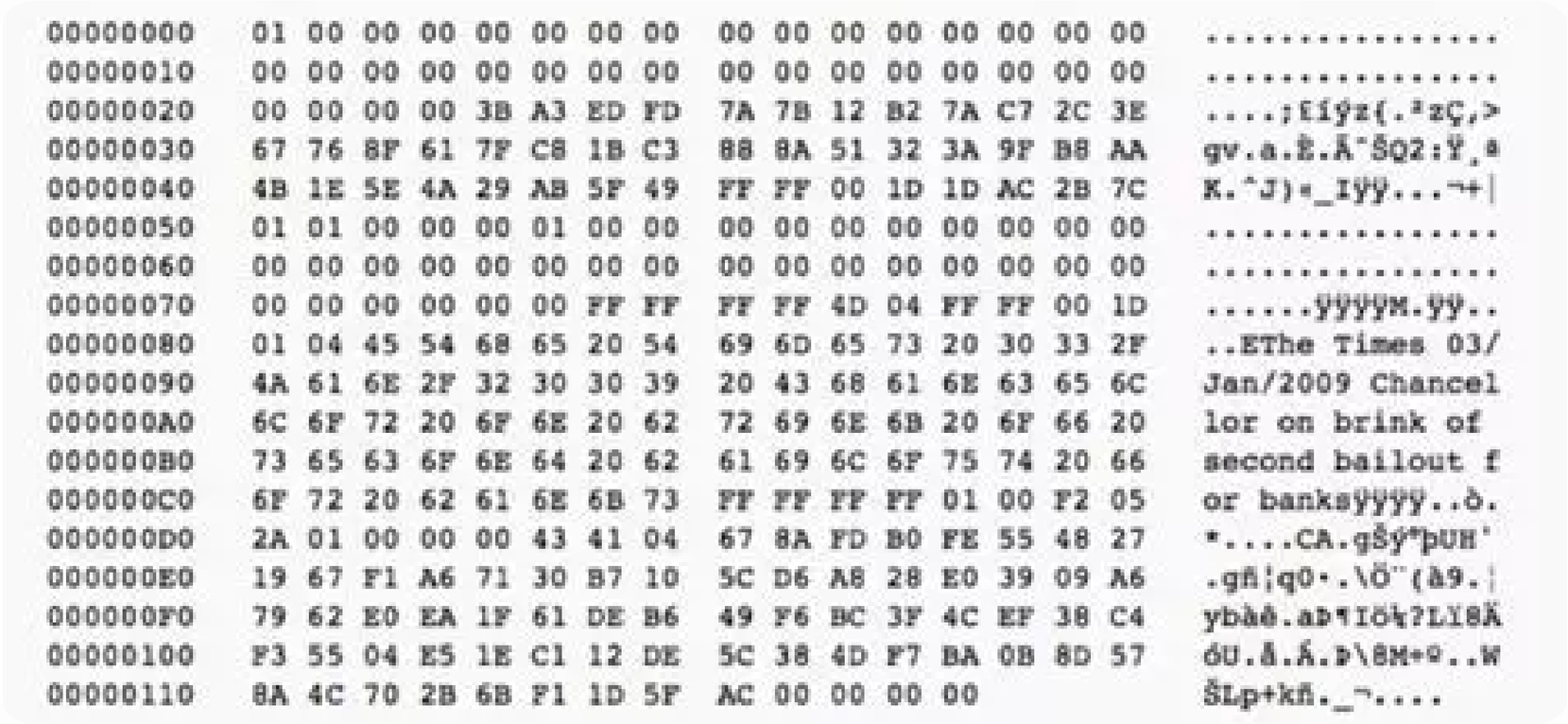
CONTRÔLE EXPORT
CATÉGORIE 5 PARTIE 2 DU RÈGLEMENT DÉLÉGUÉ (UE) 2019/2199

Clé de petite taille (< 56 bits pour les algorithmes symétriques)	Exemption pour le transfert et l'exportation depuis la France	Pas de demande de licence d'exportation

CODE PÉNAL
ARTICLE 323.1

3-7 ANS DE PRISONS
100K-300K EUROS

02



```
00000000  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E  ....;£íýz{.²zÇ,>
00000030  67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA  gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040  4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C  K.^J)«_Iÿÿ...¬+|
00000050  01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D  ......ÿÿÿÿM.ÿÿ..
00000080  01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F  ..EThe Times 03/
00000090  4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C  Jan/2009 Chancel
000000A0  6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20  lor on brink of
000000B0  73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66  second bailout f
000000C0  6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05  or banksÿÿÿÿ..ò.
000000D0  2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27  *....CA.gŠý°þUH'
000000E0  19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6  .gñ¦q0·.\Ö¨(à9.¦
000000F0  79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4  ybàê.aÞ¶Iö¼?Lï8Ä
00000100  F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57  óU.å.Á.Þ\8M÷º..W
00000110  8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00           ŠLp+kñ._¬....
```

ENTER BITCOIN

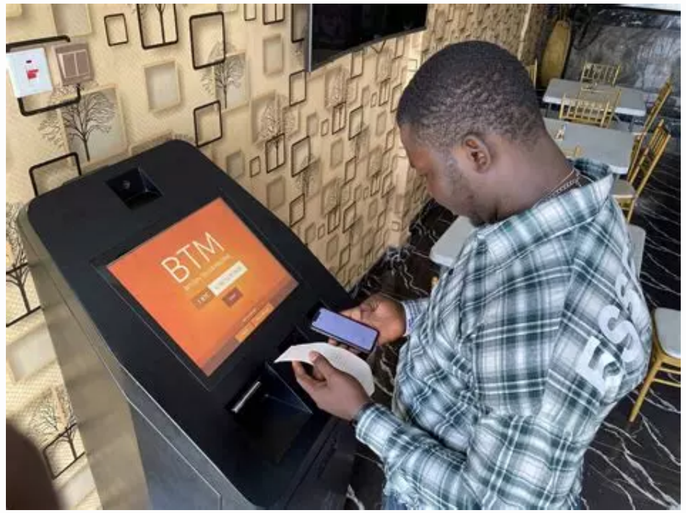
RÉVOLUTION ?

- Decentralisé
- 100% open source (code ET données)
- sécurise $2000B
- SHA256, secp256k1, ECDSA
- “rentabilise” la recherche sur la cryptographie
- 200 millions de portefeuilles

200 millions de personnes

“J’ai signé une transaction avec mon wallet”

200 millions de personnes
“J’ai signé une transaction avec mon wallet”



Africa

Salvador

Trump

Wait, What!?

Wait, What!?”

ET SI

- on signait autre chose que des transactions ?
- on enregistrait notre vie sur la blockchain ?
- on supprimait les mots de passes ?

Woleet, opentimestamp, walletconnect, account abstraction, zkp, selective disclosure, hfe, zsnark, ring signatures, etc...

03

APPROCHE VAULTYS

Fixing Internet Security

Decentralized, Passwordless Authentication

#SIMPLE #SECURE #SOVEREIGN

Mais

C’EST DUR !

Cycle de vie sur Internet en 1 slide

Avant

01 Je créé une adresse email chez un fournisseur

02 Je m’enregistre sur plein de sites avec mon email

03 Mon entreprise me donne un autre email

04 Je m’enregistre sur plein de sites avec mon email d’entreprise

05 Je pars de mon entreprise, mon email perso s’est fait piraté, je me fait bannir, mon pays en guerre avec mon fournisseur d’email, un des sites s’est fait piraté, mes mots de passes ont fuités

Après

01 Je créé mon identité numérique (ou plusieurs)

02 Je m’enregistre sur plein de sites avec mon identité

03 Je m’enregistre dans mon entreprise avec mon identité

04 Je m’enregistre sur plein de sites avec mon identité

05 Je pars de mon entreprise, mon email perso s’est fait piraté, je me fait bannir, mon pays en guerre avec mon fournisseur d’email, un des sites s’est fait piraté, ~~mes mots de passes ont fuités~~

Cycle de vie sur Internet en 1 slide

Mon identité
=
- Emails, tels, cartes bleues
- pages X, Facebook, TikTok...
- Olvid, Signal, Whatsapp
- clefs PGP
- etc...

Fail

Mon identité
=
clef publique

LES 10 PRINCIPES DU SSI

C. ALLEN 2016

https://github.com/WebOfTrustInfo/rwot2-id2020/blob/master/topics-and-advance-readings/the-path-to-self-sovereign-identity.md

01 Independent Existence

02 Full control

03 Simple Access

04 Transparent algorithm

05 Long term persistence

06 Portability

07 Interoperability

08 Consent

09 Minimalization

10 Protection

04

PROBLÈMES

PROBLÈME 0
C2C vs C2B ?

SOLUTION
C2B

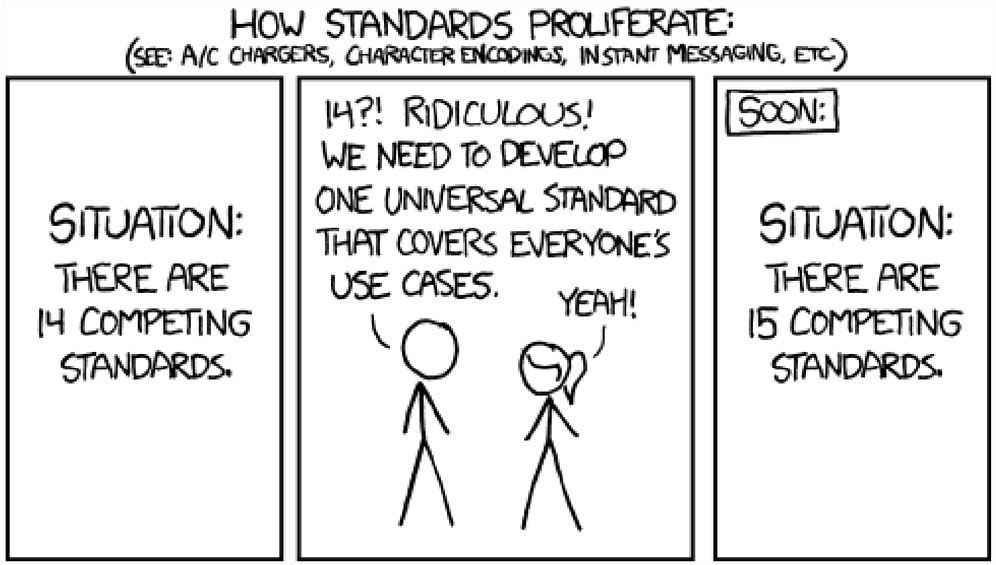
PROBLÈME 1

Comment créer/gérer son identité numérique

SOLUTION

Wallet

Merci Bitcoin



PROBLÈME 1BIS

W3C DiD et VC ne concerne pas le web of trust et n'interopère pas avec.
Pas d'interoperabilité Webauthn

SOLUTION

Nouveau protocole assurant la compatibilité de façon dégradée

json+messagepack(+saltpack)+Webauthn bridge

other takes :

- didcomm V2
- nostr connect NIP26
- ln connect

pas compatible Webauthn, pas de double auth

PROBLÈME 2

- Un wallet c’est compliqué
- Révocation de clefs ?
- Il faut acheter des jetons
- D’abord fait pour des transactions financières...
- pleins de scam !

SOLUTION

- Wallet dédié qui gère une identité auto révocable (Brevet FR3147922)
- Pas de blockchain
- Pas de jetons
- Compatible avec les standard navigateurs
  - Cryptographie, WebAuthn compatible ext. PRF
  - Passkeys, clefs FIDO2
  - https, WebRTC

PROBLÈME 2BIS

UX pour le commun des mortels

SOLUTION

2 ans de R&D pour l’UX

Encrypted

```
lPD+NWOdR4Hil6tbrBERH7ILfNa5HsOpHBNojW1OrHk2u6ala6Fm
nia6lJeSM20247oMA3JyJXAWabKyWDrX4Zdp1mynBpFQP8NlnBKJ
+W3pTV6ZkeJB/TVu/6BVUcqABYQMjpdbgsqz/pftGRSjZCBhhY+c
AIUuCJx7gq0usbtaXXOdPDTYcv2DJXS9qDPro/63KU7AFFVRdIF9
uUjGrKF6iHWMlLh4T7BbHQ66TE3Y740jp3otahimtgKQPEy2z1pP
YGs9pBKxYCE0i0Zzq9BlhAdkoaFXCtcRrN1EDm3y8QmTJ0DxiKHN
3pNwjk437xCvdIMER37D7aqJxkoFG1NPnLhnjnqXdZlh56ggy3l4
qJjh3SArvVvyd6aeqvJnKOFSxcvOhfu3EhidtenlPgap4fpOlRx0
SyAtShKY+C9TvJoJct9Ik0/3MZHOVfHJ8zI0TbtNeyI61g+vRfjQ
2WLQ8F/FG0z6eZFDQjkFj8xLdofxPsfeJc0krTkQd+OfdwuMeWKV
l3JAD1yRG903TDlO/2xkXp70p/imSKeJe438oSeg7xcxEbjwXbM/
mbwcKvoLXQ5rhbg1tVFFLAtZBSIICpM+WcoWIZemwWW8/2DavsXi
U0ISwEAityOvAqrLtaL+on4vevRd5h0yob6K20+K+G68K7tIaROL
Vvah2iYvcvzq8S8QjzZyATc=
```

Decrypted


```
{
  "protocol": "p2p",
  "service": "auth",
  "timestamp": 1736441335010,
  "pk1": "AYShdgChcMUAIImBucXIuv3A5F/VMUbYufXN5JP0hsOf
  "pk2": "AIShdgChcMUAILJJuqVY+FA22lM5TUH0krg5Em1deheo
  "nonce": "Ik84rwNOp/YEBnvTmy2KdcvQYBiqPumtwqVIrddGGn
  "sign1": "FdZe06LOjTppmyuFPG1Qlg2LUogsw2IZ7cQTkpRBcW
  "sign2": "coBwKo9mmmrRQPxMAQt3KHilMxQIp2+dO05FsY8eDl
  "metadata": {}
}
```


https://docs.vaultys.com/docs/develop/try/simulation

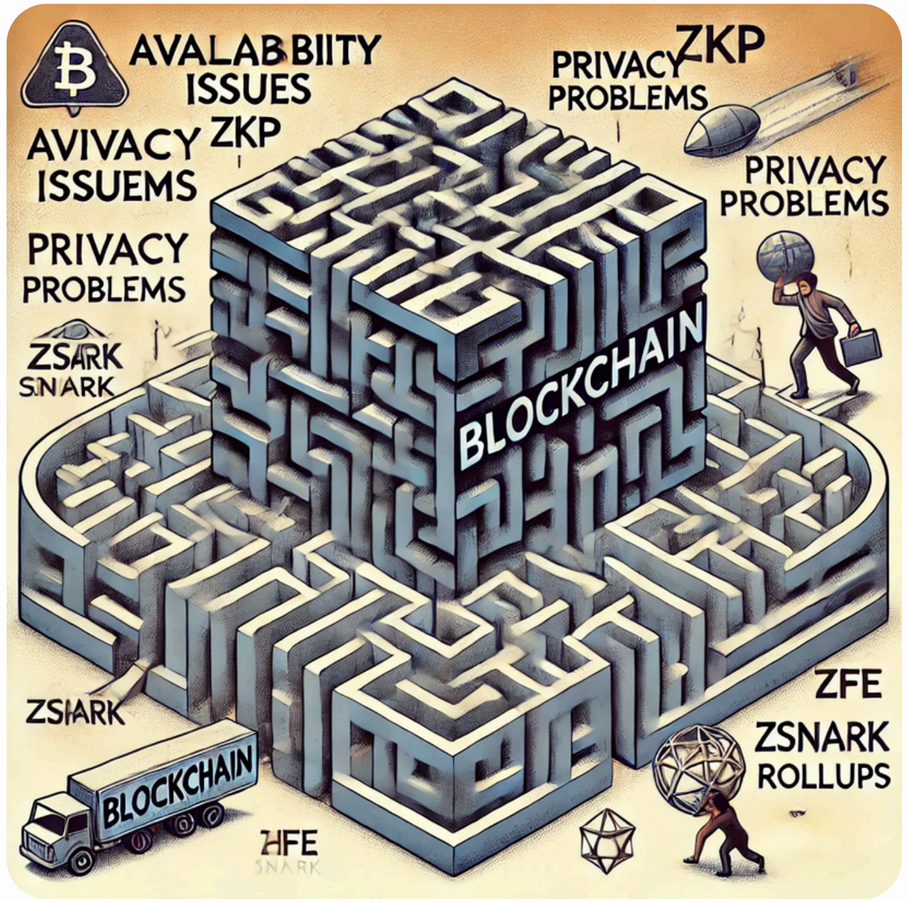
PROBLÈME 3

Signing party sérieux ? A l'ère du mobile ?!

SOLUTION

- Protocol Trust setup similaire à TLS
- Audité par Amossys
- Open-source

AMOSSYS



Yup, this one was made by chatGPT

PROBLÈME 3BIS

Blockchain

- problèmes de vie privée
  - ZKP, zsnark, HFE
  - Trèèèèèès expérimental
- problèmes de disponibilité
  - sidechain, rollups, distributed storage

SOLUTION

Pas de blockchain

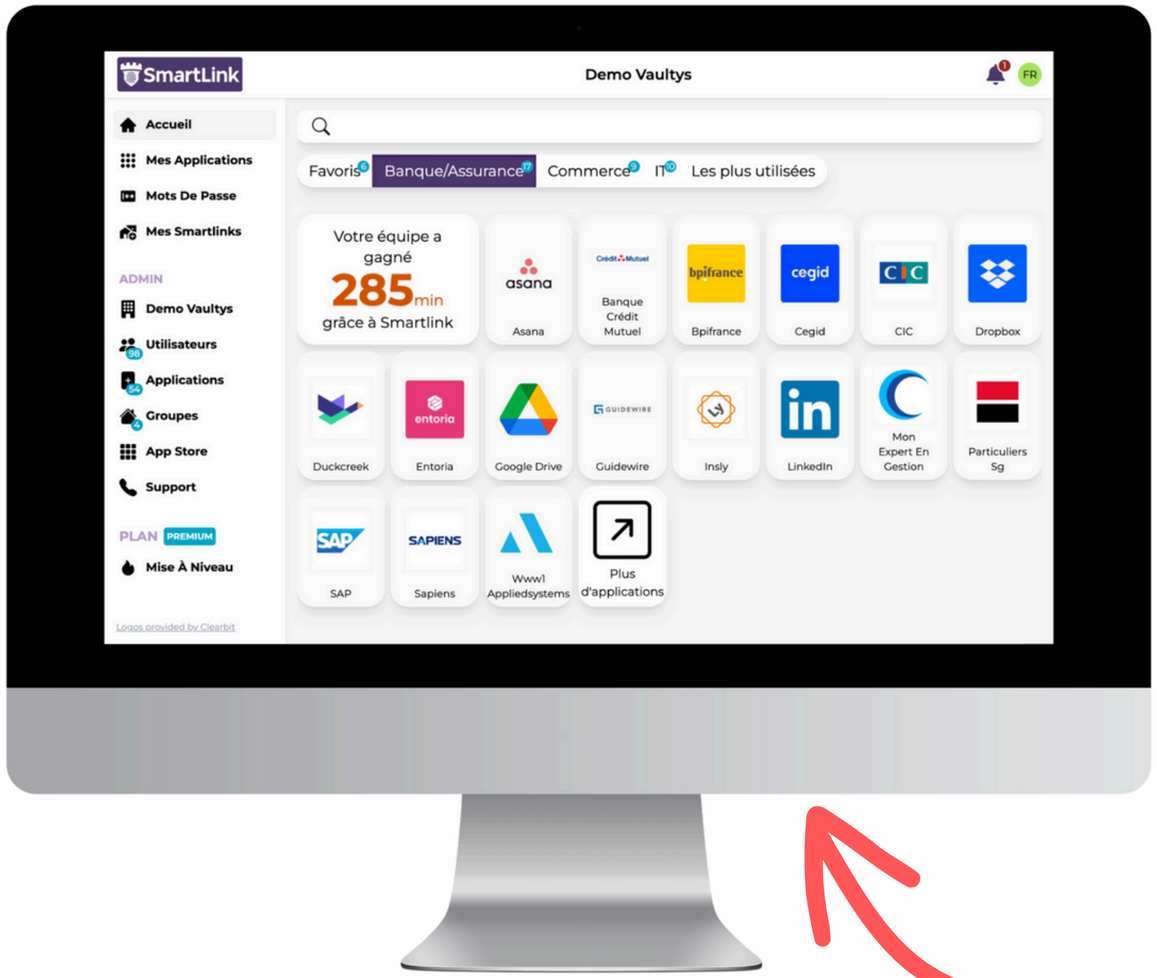
- Stockage du web of trust laissé à l’implémentation
- En pratique: stockage simple chez le propriétaire de l’identité
- Pas de garantie d’unicité d’autres données que la clef publique ailleurs que le WOT local

PROBLÈME 4

Comment se connecter à une app

SOLUTION

- Wallet dédié en cours de CSPN
- Protocole similaire au trust setup (améliorable)
- indépendant du moyen de communication
  - https, webrtc, nostr, airgap
  - Bring Your Own Communication Layer



PROBLÈME 4BIS

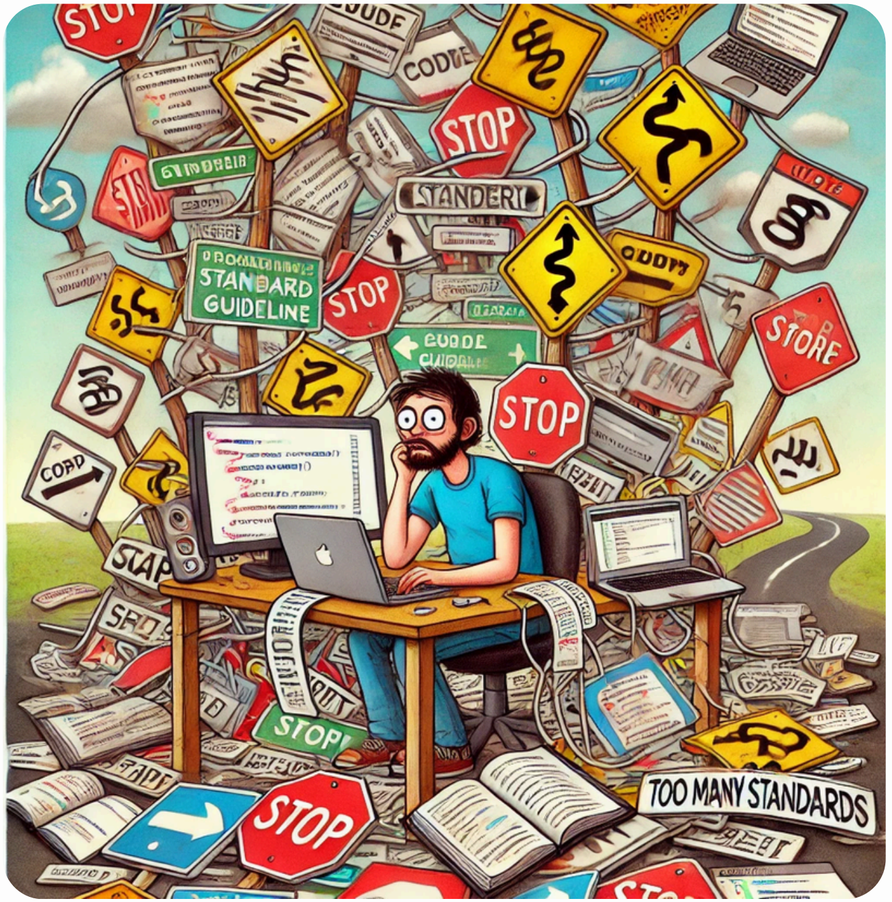
Mais ce n’est pas standard !

SOLUTION

- Smartlink pour entreprise
  - Oauth2, Saml v2, Password manager
  - Couche authentification est décentralisée

dIcAM

(decentralised) Identity and (centralised) Access Management



by chatGPT

PROBLÈME 5

Risque de fragmentation technologique

SOLUTION

- VaultysID Free
- protocole et librarie opensource soon™
- Brevet FR3147922 défensif et open-source bientôt donné à COPA
- Pas de business model autour de l’intermédiation... changement de paradigme dans la sécurité

by chatGPT

PROBLÈME 6

- Changement de responsabilité
- L’utilisateur est responsable de son identité numérique
- Je ne veux pas utiliser mon smartphone pour un truc pro

SOLUTION

- Information : La cybersecurité c’est l’affaire de tous
- Accompagnement au changement
- Proposition d’alternative (VaultysId sur le poste)

by chatGPT

PROBLÈME 7

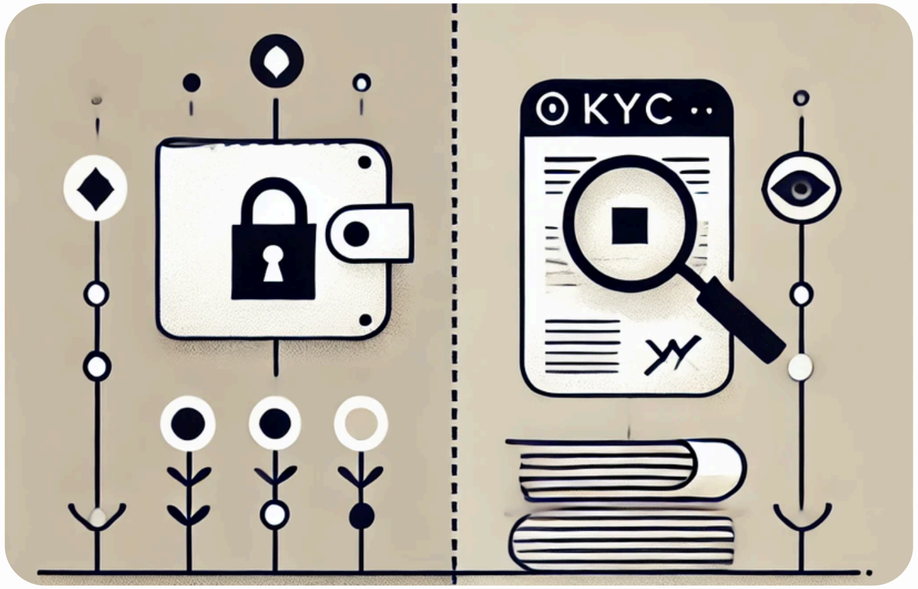
On va être tracé par l’application !

SOLUTION

- pas un service KYC/AML
- pas de compatibilité avec EBSI by design

Transition parfaite pour la conclusion

05



IDENTITY VS KYC

please clap 👏

Smart-contractualisation de la société

Veut-on créer une société qui pilote l’identité légale comme une machine ?

FRANÇOIS-XAVIER THOORENS

fx.thoorens@vaultys.com

07 44 80 78 44