GNU Anastasis

MVP Demonstration

funded by

anastasis.lu
anastasis-sarl@twitter

Florian Dold &
Christian Grothoff
{dold,grothoff}@anastasis.lu

The Problem Illustrated

nine.com.au 9NEWS

News / Technology

Man who forgot password on brink of losing $300m Bitcoin fortune

By Mark Saunokonoko • Senior Journalist | 11:45am Jan 13, 2021

U.S. NEWS

$190 Million in Cryptocurrency Missing Due t

Cryptocurrency is rarely out of the news, but the recent case involving exchange QuadrigaCX is a real show

Jack Turner | February 5th 2019 - 10:57 am

Man who can't remember password stands to lose $220 million bitcoin cache

By DAVID MATTHEWS
NEW YORK DAILY NEWS |

Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes

Bitcoin owners are getting rich because the cryptocurrency has soared. But what happens when you can't tap that wealth because you forgot the password to your digital wallet?

THE PROBLEM TECHNICALLY

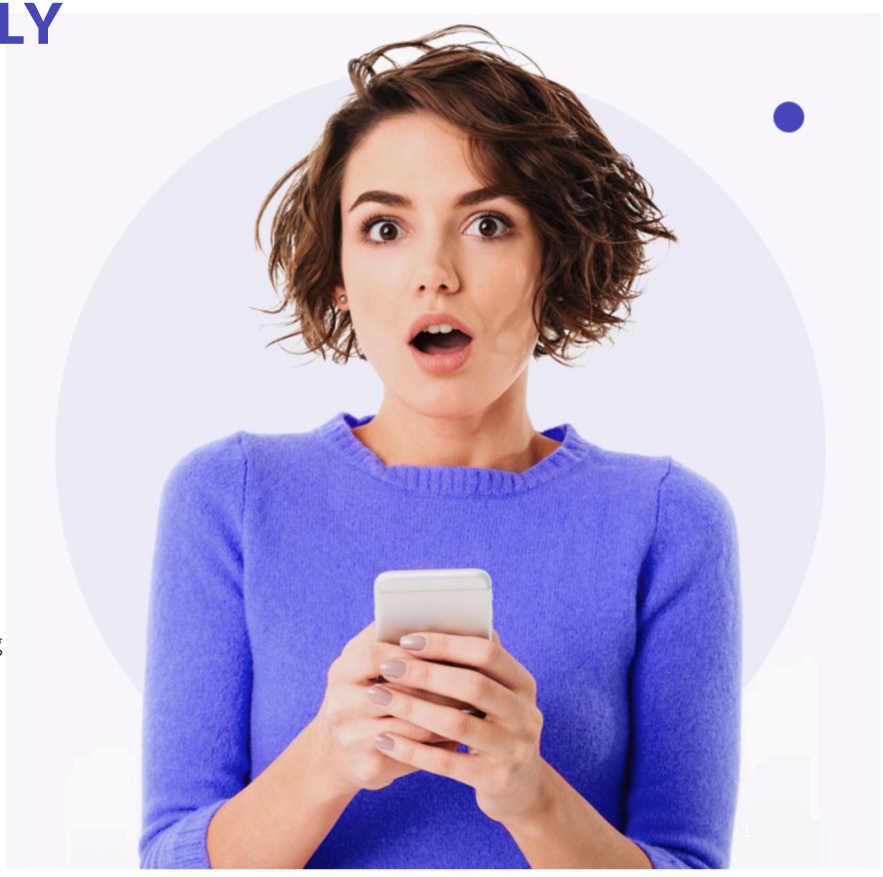
Confidentiality requires only consumer is in control of key material. Or in other words, nobody can access your password or secret key.

Consumers are unable to simultaneously ensure confidentiality and availability of keys.

Cryptographic key-splitting solutions so far are not usable.

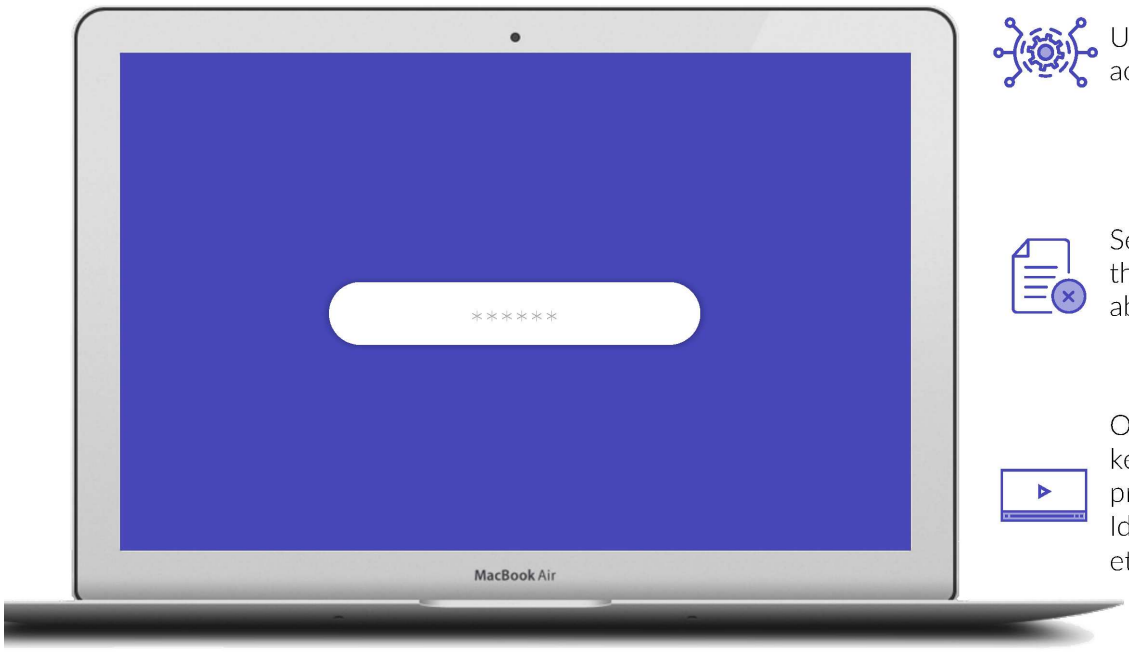
Regulation[1] forces European e-money issuers using electronic wallets to enable consumers to always recover their electronic funds (i.e. if devices are lost).

[1] According to ECB



WHAT IS ANASTASIS?

ANASTASIS IS A SECRET/KEY RECOVERY SERVICE WITH FREE & OPEN SOURCE SOFTWARE TO BACK-UP YOUR SECRET WITHOUT DEPENDING ON ANY 3rd PARTY



Users split their secret keys across multiple service providers

Service providers learn nothing about the user, except possibly some details about how to authenticate the user

Only the authorized user can recover the key by following standard authentication procedures (SMS TAN, Video-Identification, Security Question, eMail, etc.)

Software architecture overview

https://github.com/LedgerProject/Anastasis

Anastasis is a protocol.

The software consists of three components:

anastasis	Backend and client libraries (C)
anastasis-gtk	Gtk+ front-end (C)
anastasis-ts	Alternative front-end (TS) [WiP]

Major dependencies include:

GNU Taler	Privacy-preserving payments (C/TS)
Postgres	Backend database (C)
libeufin	Alternative access to banking infrastructure (Kotlin)
GNUnet	Various utility functions (C)
GNU MHD	HTTP server library (C)

Binary installation instructions

https://docs.anastasis.lu/

Debian 11:

```
# echo 'deb https://deb.taler.net/apt/debian/ bullseye main'\
  > /etc/apt/sources.list/taler.list
# wget -O - https://taler.net/taler-systems.gpg.key |\
  apt-key add -
# apt update
# apt install anastasis-gtk
```

Ubuntu 20.04:

```
# echo 'deb https://deb.taler.net/apt/ubuntu/ focal-fossa main'\
  > /etc/apt/sources.list/taler.list
# wget -O - https://taler.net/taler-systems.gpg.key |\
  apt-key add -
# apt update
# apt install anastasis-gtk
```

Do you have any questions?

https://anastasis.lu/

References:

1. Dennis Neufeld and Dominik Meister. *Anastasis: Password-less key recovery via multi-factormulti-party authentication*. **BFH, 2020**.
2. David Chaum, Christian Grothoff and Thomas Moser. *How to Issue a Central Bank Digital Currency*. **Swiss National Bank Working Papers, 3/2021**
3. Florian Dold. *The GNU Taler System: Practical and Provably Secure Electronic Payments*. **University of Rennes 1**, 2019.