GNUnet & NGI

Christian Grothoff

23.11.2021

Overview

Context

Design Choices for a Civil Network!

Internet Design Goals (David Clark, 1988)

1. **Internet communication must continue despite loss of networks or gateways.**
2. The Internet must support multiple types of communications service.
3. The Internet architecture must accommodate a variety of networks.
4. The Internet architecture must permit *distributed management* of its resources.
5. The Internet architecture must be cost effective.
6. The Internet architecture must permit host attachment with a low level of effort.
7. **The resources used in the internet architecture must be accountable.**

GNUnet Design Goals

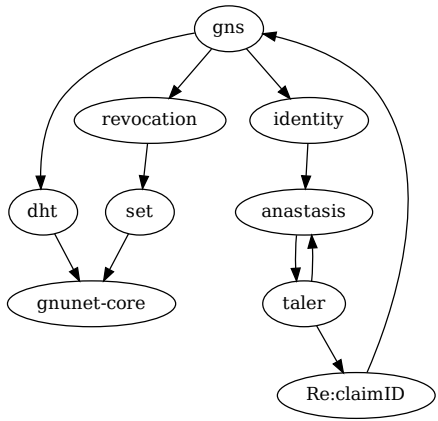
1. GNUnet must be implemented as Free Software.
2. GNUnet must minimize the amount of personally identifiable information exposed.
3. The GNUnet must be fully distributed and resilient to external attacks and rogue participants.
4. GNUnet must be self-organizing and not depend on administrators or centralized infrastructure.
5. GNUnet must inform the user which other participants have to be trusted when establishing private communications.
6. GNUnet must be open and permit new peers to join.
7. GNUnet must support a diverse range of applications and devices.
8. GNUnet must use compartmentalization to protect sensitive information.
9. The GNUnet architecture must be resource efficient.
10. GNUnet must provide incentives for peers to contribute more resources than they consume.

Applications in GNUnet (under development)

- Anonymous and non-anonymous publishing (**NGI DISCOVERY**[1])
- IPv6–IPv4 protocol translation and tunnelling
- Conversation: secure, decentralized voice communication
- **GNU Name System**: censorship-resistant replacement for DNS (**NGI DISCOVERY**)
  - Revocation: Key revocation via Set Reconciliation (Elias Summermatter)
  - Ascension: Automatically migrate DNS zones to GNS (Patrick Gerber)
- Re:claimID: identity management (**NGI TRUST**)
- **GNU Taler**: privacy-friendly payments (**NGI ZERO, NGI POINTER**)
- **GNU Anastasis**: key escrow and recovery (**NGI LEDGER**)

[1] ERIS

Software Architecture



System Architectures

GNUnet	Fully decentralized, peer-to-peer ⇒ DHT
Re:claimID	Self-sovereign identities with trusted authorities for attestation
GNU Anastasis	Client-side secret splitting, untrusted multiple servers in Clouds
GNU Taler	Classical client-server

The GNU Name System

Back to the Internet: DNS troubles

- DNS remains a source of traffic amplification for DDoS
- DNS censorship (i.e. by China) causes collateral damage in other countries
- DNS is part of the mass surveillance apparatus (MCB)
- DNS is abused for the offensive cyber war (QUANTUMDNS)

Band aid solutions[2] will **not** fix this.

[2] DNS-over-TLS, DoH, DNSSEC, DPRIVE, ODNS, ...

The GNU name system

- Decentralized name system
- Supports globally unique (& secure) identification
- Achieves query and response privacy
- Provides public key infrastructure
- Virtually instant key revocation
- Interoperable with DNS

Applications for GNS

DNS	Theoretical full replacement ($\Rightarrow$ Ascension)
SecuShare	PKI for decentralized social networking applications (Carlo von Loesch, et al)
Re:claimID	OIDC-compatible provider-less identity management / SSO platform
p≡p	PKI for e-mail

GNUnet – R^5N

Distributed Hash Tables (DHTs)

- Distributed **index**
- GET and PUT operations like a hash table
- JOIN and LEAVE operations (internal)
- Trade-off between JOIN/LEAVE and GET/PUT costs
- Typically use exact match on cryptographic hash for lookup
- Typically require overlay to establish particular connections

Assessing DHTs

- Performance?
- Security against Eclipse attack?
- Survivability of DoS attack?
- Maintenance operation cost & required frequency?
- Latency? ($\neq$ number of hops!)
- Data persistence / replication?

Interesting R^5N properties

- Kademlia-style XOR distance metric is symmetric: connections are used in both directions
- Replication helps with malicious peers and churn
- Recursive lookup supports networks with restricted, link-encrypted communication between peers
- Lookup helps with routing table maintenance
- Bucket size trade-off between routing speed and table size
- Randomization to defeat censorship attack
- Content-validation to defeat pollution attacks
- Route tracking enables use of DHT to build routing tables for messaging applications

Our NGI Trust project: Scope

- RFC-style specification of the R^5N protocol
- Improvement of route tracking security
- Generalization to non-GNUnet underlays
- Adaptation of existing C, JavaScript implementations to specification
- Re-implementation in Go

Our NGI Trust project: Status

- Started specification work
  $\Rightarrow$ discussion discovered bugs in C implementation
- Started non-GNUnet underlay
  $\Rightarrow$ API design maybe OK
  $\Rightarrow$ sketchy, untested first implementation
- Go developer developed health issues instead of software

GNU Anastasis

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

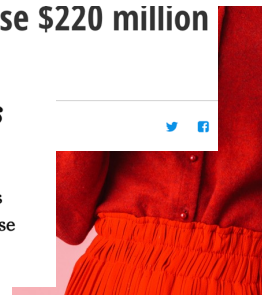
Jack Turner | February 5th 2019 - 10:57 am

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

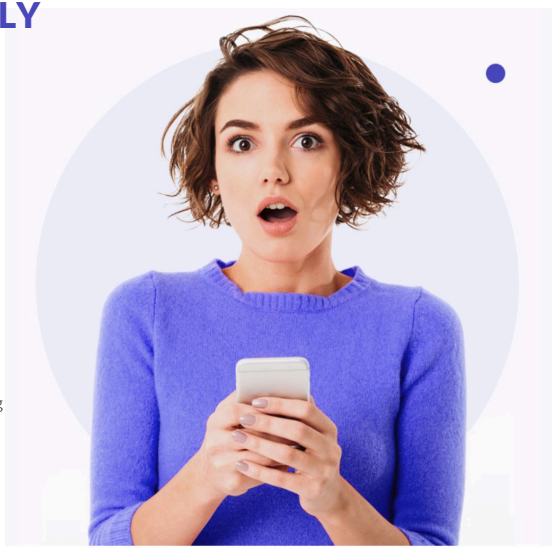
Confidentiality requires only consumer is in control of key material. Or in other words, nobody can access your password or secret key.

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

Cryptographic key-splitting solutions so far are not usable.

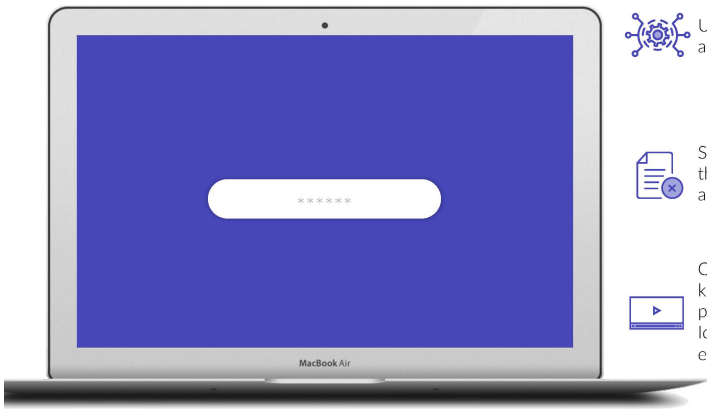
Regulation[1] forces European e-money issuers using electronic wallets to enable consumers to always recover their electronic funds (i.e. if devices are lost).

[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.)

Design principles

GNU Anastasis must ...

1. ... be Free Software[3]. Everyone must have the right to run the program, study the source code, make modifications and share their modifications with others.
2. ... not rely on the trustworthiness of individual providers. It must be possible to use Anastasis safely, even if a subset of the providers is malicious. Anastasis must minimize the amount of information exposed to providers and the network.
3. ... put the user in control: They get to decide which providers to use, and which combinations of authentication steps will be required to restore their core secret. The core secret always remains exclusively under the user's control, even during recovery.
4. ... be economical viable to operate. This implies usability and efficiency of the system.
5. ... support a diverse range of use cases.

[3] `https://www.fsf.org/`

GNU Taler

A Social Problem

This was a question posed to RAND researchers in 1971:

> *"Suppose you were an advisor to the head of the KGB, the Soviet Secret Police. Suppose you are given the assignment of designing a system for the surveillance of all citizens and visitors within the boundaries of the USSR. The system is not to be too obtrusive or obvious. What would be your decision?"*

A Social Problem

This was a question posed to RAND researchers in 1971:

> *"Suppose you were an advisor to the head of the KGB, the Soviet Secret Police. Suppose you are given the assignment of designing a system for the surveillance of all citizens and visitors within the boundaries of the USSR. The system is not to be too obtrusive or obvious. What would be your decision?"*

Mastercard/Visa are too transparent.

"I think one of the big things that we need to do, is we need to get a way from true-name payments on the Internet. The credit card payment system is one of the worst things that happened for the user, in terms of being able to divorce their access from their identity." –Edward Snowden, IETF 93 (2015)

What is Taler?

https://taler.net/en/features.html

Taler is

- a Free/Libre software *payment system* infrastructure project
- ... with a surrounding software ecosystem
- ... and a company (Taler Systems S.A.) and community that wants to deploy it as widely as possible.

However, Taler is

- *not* a currency
- *not* a long-term store of value
- *not* a network or instance of a system
- *not* decentralized
- *not* based on proof-of-work or proof-of-stake
- *not* a speculative asset / "get-rich-quick scheme"

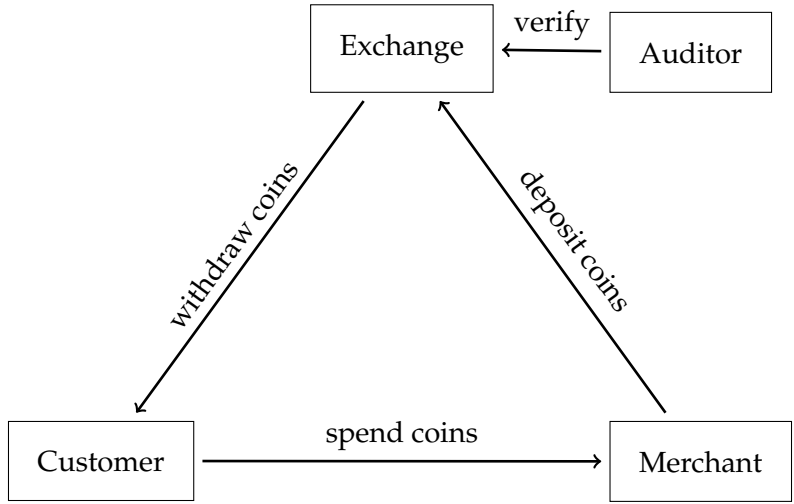
Design principles

https://taler.net/en/principles.html

GNU Taler must ...

1. ... be implemented as **free software**.
2. ... protect the **privacy of buyers**.
3. ... must enable the state to **tax income** and crack down on illegal business activities.
4. ... prevent payment fraud.
5. ... only **disclose the minimal amount of information necessary**.
6. ... be usable.
7. ... be efficient.
8. ... avoid single points of failure.
9. ... foster **competition**.

Taler Overview



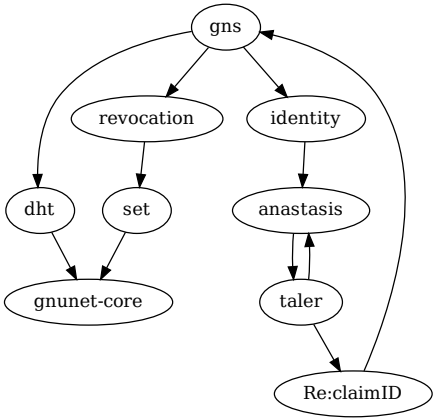
GNUnet and the NGI

Completed work within NGI

NGI DISCOVERY RFC-style protocol specification for GNS, 2nd implementation in Go, GNUnet packages for major distributions (done)

NGI TRUST Attribute attestation for Re:claimID, integrated demonstrator with Taler and WooCommerce to provide account-less form-less shopping experience; usability study

NGI ZERO Security audit of GNU Taler and Taler auditor deployment preparations



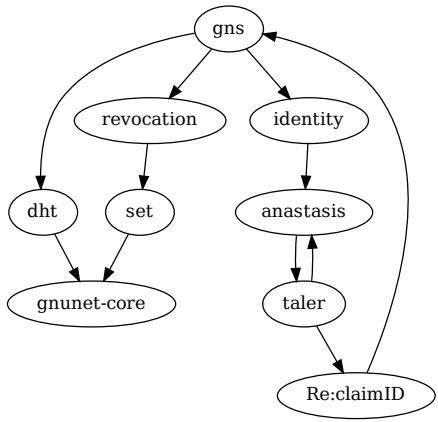
Ongoing work

NGI ASSURE R^5N DHT RFC-style protocol specification, multi-language implementation, underlay abstraction, security improvements, underlay abstraction for DHT

NGI ASSURE Layer2Overlay: NAT traversal, pluggable, uni-directional transports, self-configuration

NGI Fed4Fire+ GNU Taler scalability for Digital Euro in Grid5000

NGI LEDGER Anastasis multi-language implementation, integration with GNU Taler, many-factor authentication and business creation



Future work

- Enhance $p \equiv p$ to create foundation for P2P payments via e-mail:
  - Fog of trust instead of Web of trust
  - Reunion key exchange
  - Ryge's triangle for key managmenet
  - Anastasis & Taler integration
- Enhancements to Taler:
  - IoT (scale-down wallet resource requirements)
  - Media companies (more expressive contracts)
  - Auditor automation and scalability
- SMC for cosine similarity for collaborative filtering in news distribution
- Modernize GNU libmicrohttpd – `https://www.gnu.org/s/libmicrohttpd/`

Help needed

- Marketing:
  - GNU Anastasis – `https://anastasis.lu/` & `https://www.gnu.org/s/anastasis/`
  - GNU Taler – `https://taler-systems.com/` & `https://taler.net/`
  - Reclaim:ID – `https://reclaim.gnunet.org/`
- Translations:
  - Websites
  - Applications
  - Documentation

Key publications

- Martin Schanzenbach, Christian Grothoff, Bernd Fix. *The R5N Distributed Hash Table*. `https://lsd.gnunet.org/lsd0004/`, 2021+
- Martin Schanzenbach, Christian Grothoff, Bernd Fix. *The GNU Name System*. `https://datatracker.ietf.org/doc/draft-schanzen-gns/`, 2021
- Martin Schanzenbach, Christian Grothoff, Hansjürg Wenger and Maximilian Kaul. *Decentralized Identities for Self-sovereign End-users (DISSENS)*. Open Identity Summit 2021
- David Chaum, Christian Grothoff and Thomas Moser. *Comment émettre une monnaie numérique de banque centrale*. `https://www.snb.ch/en/mmr/papers/id/working_paper_2021_03`, 2021
- Florian Dold, Christian Grothoff. *The 'payto' URI Scheme for Payments*. `https://tools.ietf.org/html/rfc8905`, 2020

NGI Experience

- **Short** applications
- **High** success rate
- **Minimal** bureocratic overheads with **NLnet**-managed applications
- **Flexible** execution plans
- **Insane** impact potential
- **Adequate** mentoring support (but sometimes too static)

NGI Experience

- **Short** applications
- **High** success rate
- **Minimal** bureocratic overheads with **NLnet**-managed applications
- **Flexible** execution plans
- **Insane** impact potential
- **Adequate** mentoring support (but sometimes too static)

$$\sum = \textbf{best EU/EC funding program so far}$$