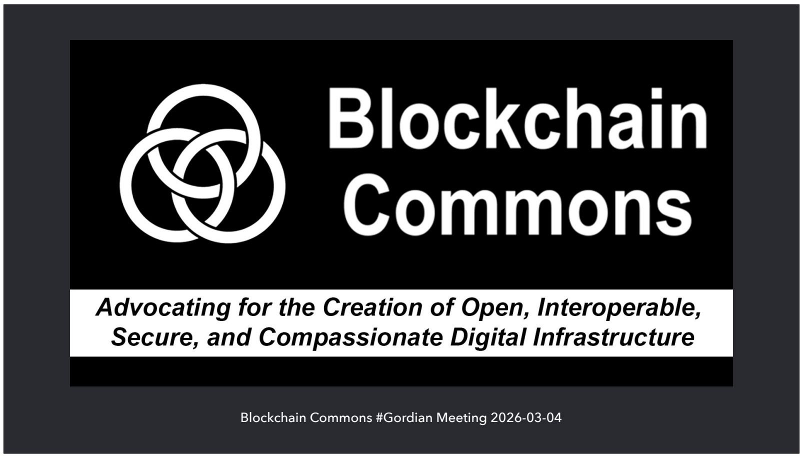


Blockchain Commons

Advocating for the Creation of Open, Interoperable, Secure, and Compassionate Digital Infrastructure

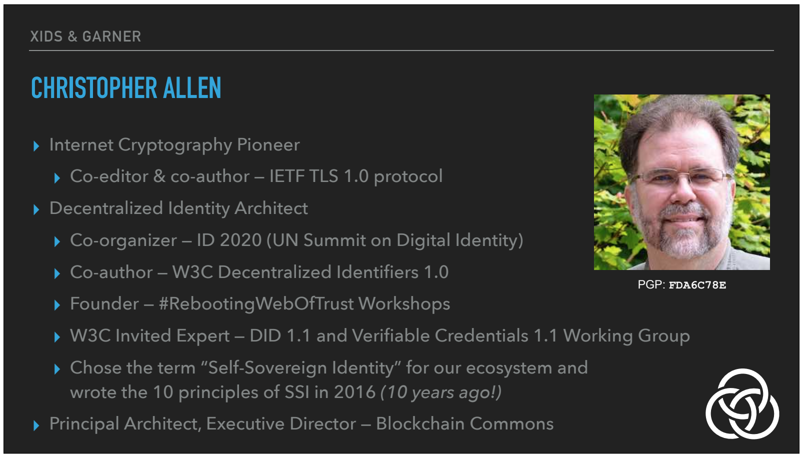
Blockchain Commons #Gordian Meeting 2026-03-04

Welcome to our meeting of the Gordian Developer Community, which we hold monthly on the 1st Wednesday of the month. Today is March 4th, 2026.

BLOCKCHAIN COMMONS

XIDS & GARNER

Today our main presentation is on the Extensible Identifier, or XID, and the Garner server. These are both technologies that we’ve created to better support self-sovereign identity.



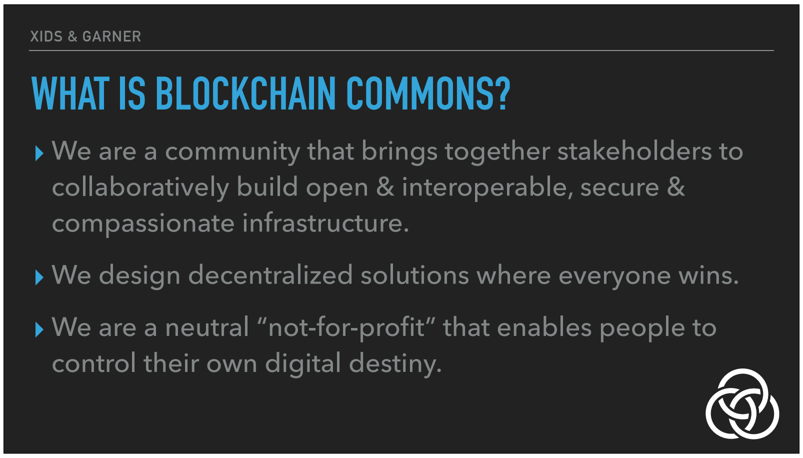
XIDS & GARNER

CHRISTOPHER ALLEN

- Internet Cryptography Pioneer
  - Co-editor & co-author – IETF TLS 1.0 protocol
- Decentralized Identity Architect
  - Co-organizer – ID 2020 (UN Summit on Digital Identity)
  - Co-author – W3C Decentralized Identifiers 1.0
  - Founder – #RebootingWebOfTrust Workshops
  - W3C Invited Expert – DID 1.1 and Verifiable Credentials 1.1 Working Group
  - Chose the term "Self-Sovereign Identity" for our ecosystem and wrote the 10 principles of SSI in 2016 *(10 years ago!)*
- Principal Architect, Executive Director – Blockchain Commons

PGP: `FDA6C78E`

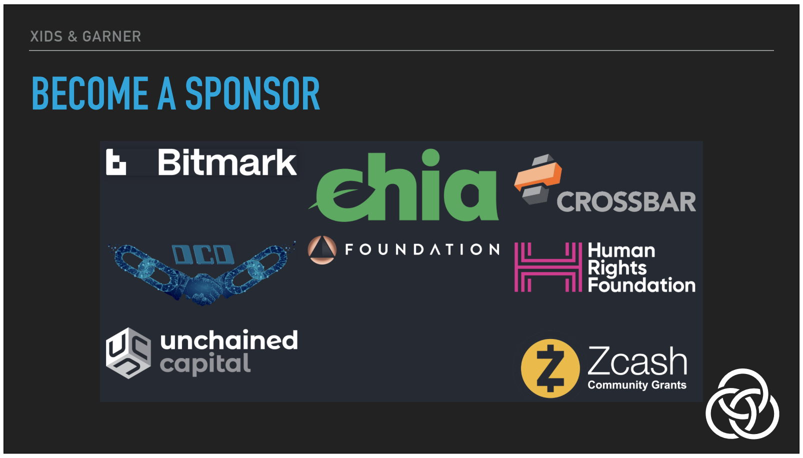
Who am I? My name is Christopher Allen. In recent years, I've been deeply involved with the architecture of the W3C Decentralized Identifier international standard. But, I feel like it's gone wrong as it's been deployed, so XIDs and Garner are some of the tools I'm working on to move DIDs back to their first principles.



WHAT IS BLOCKCHAIN COMMONS?

- We are a community that brings together stakeholders to collaboratively build open & interoperable, secure & compassionate infrastructure.
- We design decentralized solutions where everyone wins.
- We are a neutral "not-for-profit" that enables people to control their own digital destiny.

This is part of the work of Blockchain Commons, which has been broadly focused on creating independence, privacy, resilience, and openness for digital assets. We haven't done a lot of work on identity until the last year or so because we didn't have identity sponsors, but I felt like the needs were becoming so great that I had to talk about the problems with SSI more, even without funding on this topic.



XIDS & GARNER

BECOME A SPONSOR

Bitmark
chia
CROSSBAR
DCD
FOUNDATION
Human Rights Foundation
unchained capital
Zcash
Community Grants

Of course you can help us in that regard by becoming an identity sponsor. Talk to me if you'd like to become more involved in this work. (And thanks to the organizations that have helped support the wider work that Blockchain Commons does.)

BLOCKCHAIN COMMONS

NEW TECHNOLOGY VIDEO

Before we dive into some new tools for digital identity, I wanted to share with you about our 2026 technology overview video. Over the last several years, Blockchain Commons has developed numerous technologies meant to improve the independence, privacy, resilience, and openness of the internet.

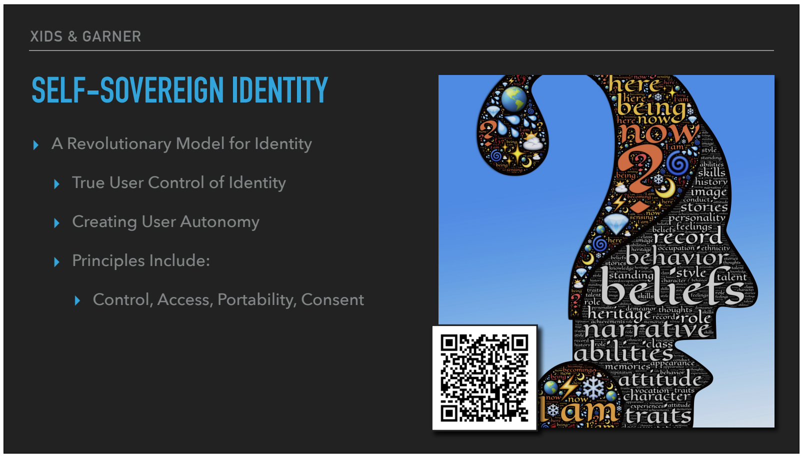
XID
EXTENSIBLE IDENTIFIERS
GARNER
GORDIAN CLUBS
YOUTUBE
HUBERT
RESEARCH REPO
FROST
GORDIAN DEV MEETING
KNOWN VALUES
PROVENANCE MARKS
GSTP
GORDIAN SEALED TRANSACTION PROTOCOL
ESC
ESC
ENCRYPTED STATE CONTINUATIONS
dCBOR
DETERMINISTIC CBOR
> dCBOR
DCBOR CLI
GORDIAN ENVELOPE
ENVELOPE CLI
MULTIPART URs (MUR)
SSKR
GORDIAN SEED TOOL
SEEDTOOL CLI
LIFEHASH
ROAD SAGA CASH NAVY
BYTEWORDS
ROAD SAGA CASH NAVY
OBJECT INFORMATION BLOCKS (OIB)
UR:
UNIFORM RESOURCES

Our brand-new 2026 Technology Overview from Blockchain Commons describes each of 24 different technologies, applications, and references, each in about a minute. It offers the most comprehensive and accessible look at our Gordian Technology tech stack to date. If you are trying to explain to you colleagues what our tools enable, this 22 minute vide is the place to start.

MAKING USER AGENCY A REALITY

SELF-SOVEREIGN IDENTITY & THE POWER OF XIDS

Alright, let’s get started on Self-Sovereign Identity itself, and how I’ve returned to first principles with XIDs.

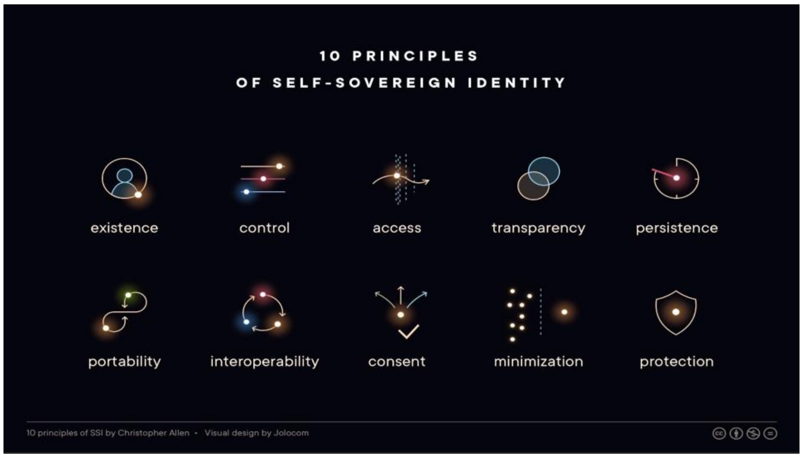


XIDS & GARNER

SELF-SOVEREIGN IDENTITY

- A Revolutionary Model for Identity
  - True User Control of Identity
  - Creating User Autonomy
  - Principles Include:
    - Control, Access, Portability, Consent

This is likely review for many of you, but the modern idea of self-sovereign identity was largely founded in an article I wrote called “The Path to Self-Sovereign Identity” just before the 2nd Rebooting the Web of Trust, which we ran in conjunction with ID2020, the first United Nation conference on digital identity. The idea was simple: digital identity is central to our online presence, thus we should control it. We are NOT digital serfs!



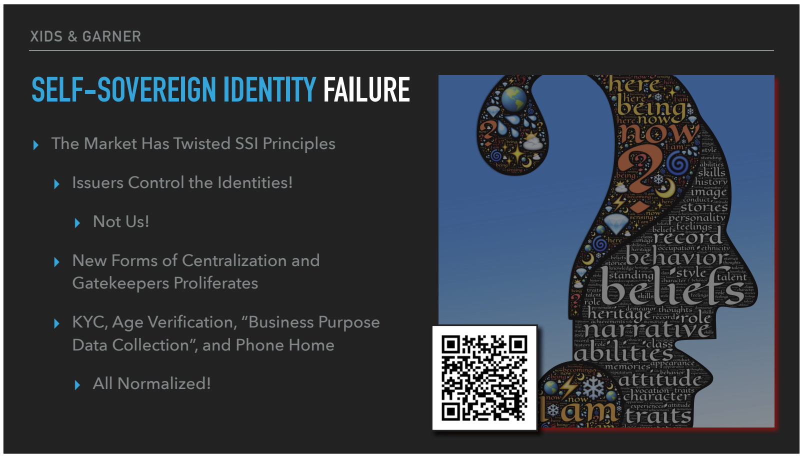
10 PRINCIPLES
OF SELF-SOVEREIGN IDENTITY

existence
control
access
transparency
persistence

portability
interoperability
consent
minimization
protection

10 principles of SSI by Christopher Allen • Visual design by Jolocom

These ten principles for Self-Sovereign Identity basically say: You, not a gatekeeper, should have total access and control over your identity. Your identity should be long-lasting, and you should have a choice in how it is used and be able to move it to different places. (That doesn't mean you can control what other people say about you, just that you control what you say!)



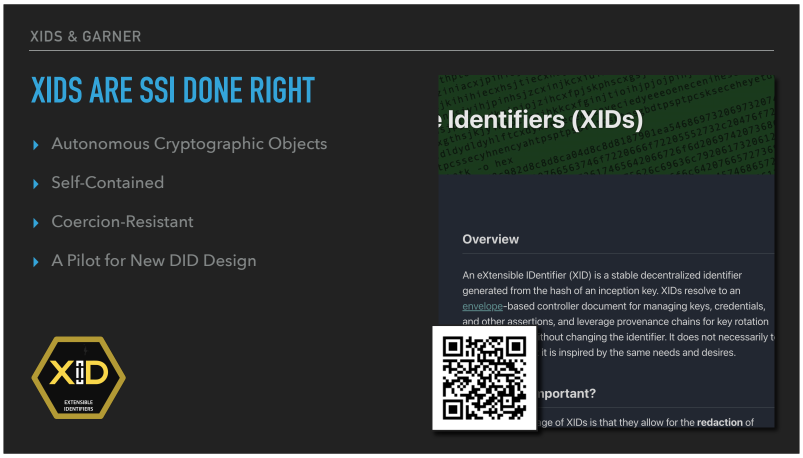
XIDS & GARNER

SELF-SOVEREIGN IDENTITY FAILURE

- The Market Has Twisted SSI Principles
  - Issuers Control the Identities!
    - Not Us!
  - New Forms of Centralization and Gatekeepers Proliferates
  - KYC, Age Verification, "Business Purpose Data Collection", and Phone Home
    - All Normalized!

here
being
now
skills
history
image
stories
personality
record
behavior
beliefs
style
talent
heritage
role
narrative
abilities
class
attitude
character
i am
traits

Unfortunately, self-sovereign identity as we imagined it back in 2016 has failed, largely due to developers neglecting the principles. Issuers have way too much control: they're the only ways to create identities, and they decide what you must reveal about your identity. They've also built centralization and even phone-home behavior into their supposedly decentralized identifiers. KYC, age verification, and collection of your data because it, quote: "has a legitimate business purpose" has become normalized.



XIDS & GARNER

XIDS ARE SSI DONE RIGHT

- Autonomous Cryptographic Objects
- Self-Contained
- Coercion-Resistant
- A Pilot for New DID Design

e Identifiers (XIDs)

Overview

An eXtensible IDentifier (XID) is a stable decentralized identifier generated from the hash of an inception key. XIDs resolve to an envelope-based controller document for managing keys, credentials, and other assertions, and leverage provenance chains for key rotation

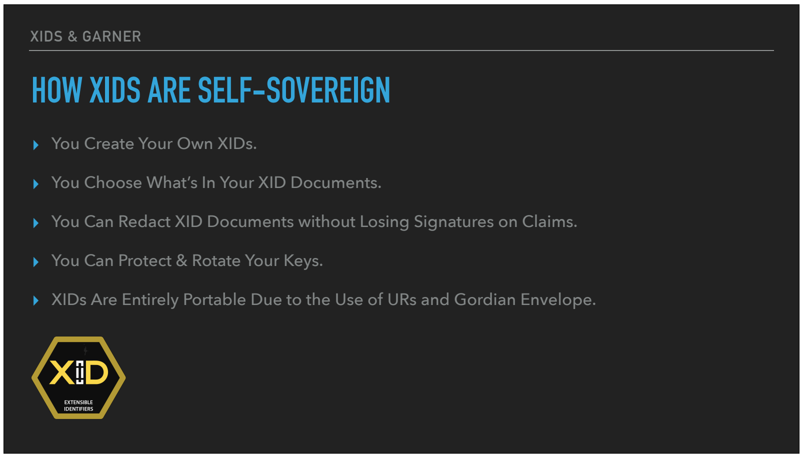
ithout changing the identifier. It does not necessarily t

it is inspired by the same needs and desires.

nportant?

age of XIDs is that they allow for the **redaction** of

I built XIDs to be a reference implementation for how self-sovereign identity could be done right. They’re totally self-contained and they’re totally controlled by the holder. No one else is involved, so there are no possibilities for centralization or outside control.



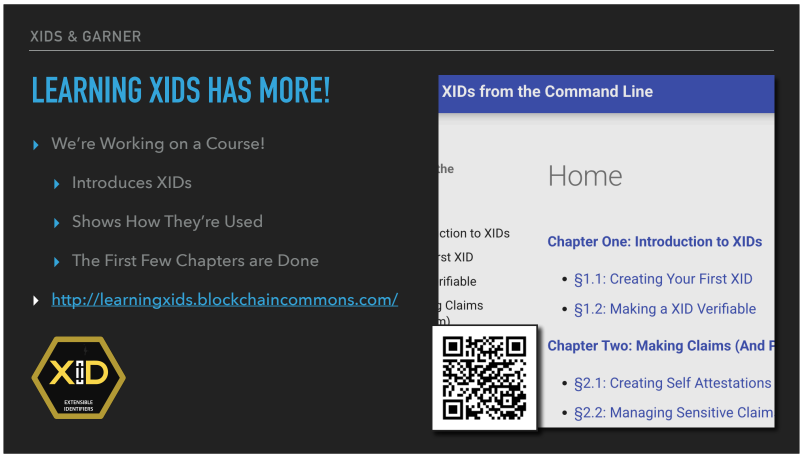
XIDS & GARNER

HOW XIDS ARE SELF-SOVEREIGN

- You Create Your Own XIDs.
- You Choose What's In Your XID Documents.
- You Can Redact XID Documents without Losing Signatures on Claims.
- You Can Protect & Rotate Your Keys.
- XIDs Are Entirely Portable Due to the Use of URs and Gordian Envelope.

XID
EXTENSIBLE IDENTIFIERS

Looking back at the principles of self-sovereign identity, XIDs ensure the holder has access, transparency, and control. They support minimization, and they're portable and interoperable as long as our low-level specifications for URs and envelopes have been adopted.



LEARNING XIDS HAS MORE!

- We're Working on a Course!
  - Introduces XIDs
  - Shows How They're Used
  - The First Few Chapters are Done
- http://learningxids.blockchaincommons.com/

XIDs from the Command Line

the

ction to XIDs

rst XID

rifiable

g Claims

m)

Home

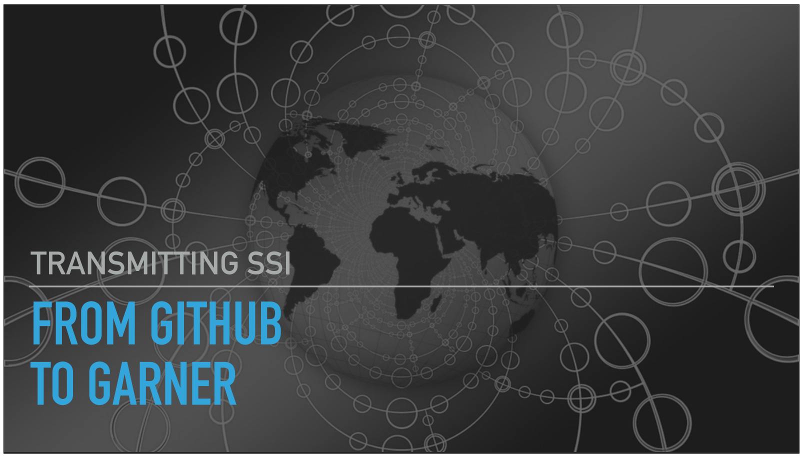
Chapter One: Introduction to XIDs

- §1.1: Creating Your First XID
- §1.2: Making a XID Verifiable

Chapter Two: Making Claims (And F

- §2.1: Creating Self Attestations
- §2.2: Managing Sensitive Claim

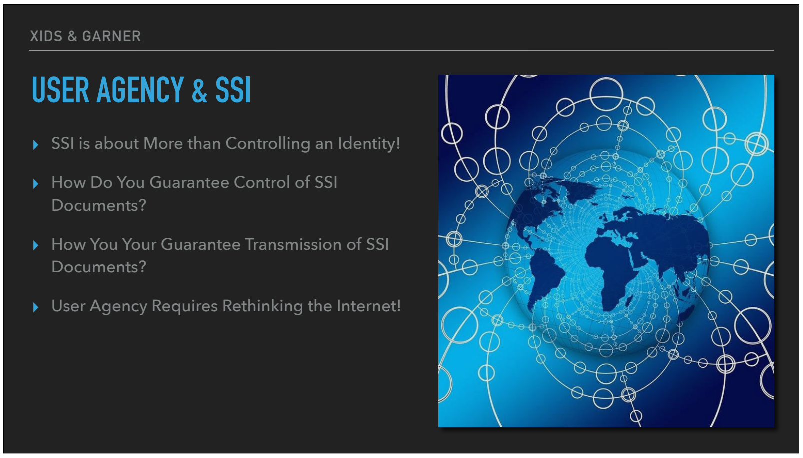
We think XIDs are very important not just as an alternative to the DID spec, but as a promise of what the DID spec could become, so we're working on a whole course called Learning XIDs from the Command Line, at learningxids.blockchaincommons.com. It follows the format of our popular Learning Bitcoin from the Command Line course.



TRANSMITTING SSI

FROM GITHUB
TO GARNER

So that’s XIDs in a nutshell, but they’re just a first step, because there’s a lot more to ensuring that self-sovereign identity truly remains self-sovereign.

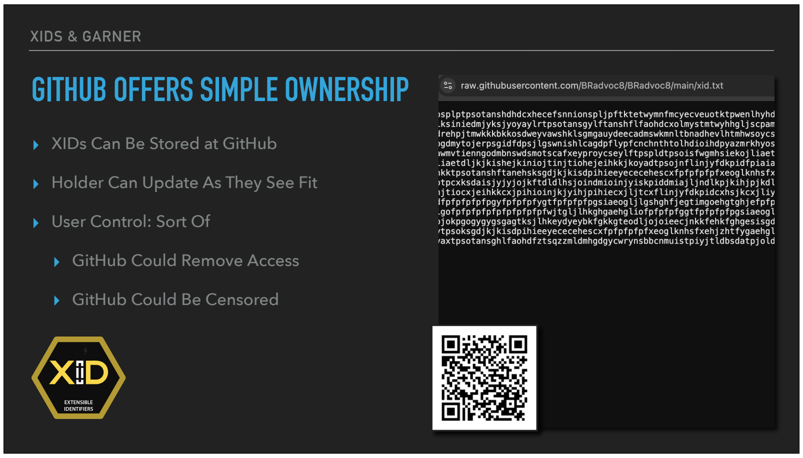


XIDS & GARNER

USER AGENCY & SSI

- SSI is about More than Controlling an Identity!
- How Do You Guarantee Control of SSI Documents?
- How You Your Guarantee Transmission of SSI Documents?
- User Agency Requires Rethinking the Internet!

You can control an identity, but how do you publish it when you might not be able to guarantee the infrastructure, which could be compromised, censored, or just absent? Assuring that your self-sovereign identity can enter into a self-sovereign network.



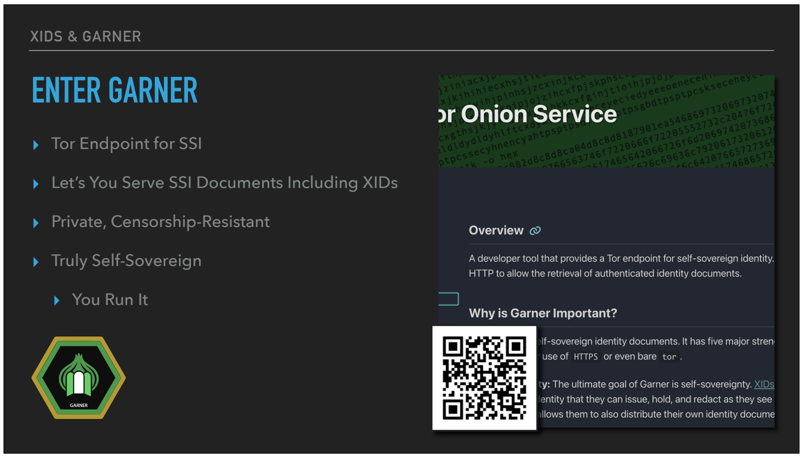
XIDS & GARNER

GITHUB OFFERS SIMPLE OWNERSHIP

- XIDs Can Be Stored at GitHub
- Holder Can Update As They See Fit
- User Control: Sort Of
  - GitHub Could Remove Access
  - GitHub Could Be Censored

```
splptpsotanshdhdcxhecefsnnionspljpftktetwymnfmcyecveuotktpwenlhyhd
ksiniedmjyksjyoyaylrtpsotansgylftanshflfaohdcxolmystmtwyhhgljscpam
rehpjtmwkkkbkkosdweyvawshklsgmgauydeecadmswkmnltbnadhevlhtmhwsoycs
gdmytojerpsgidfdpsjlgswnishlcagdpflypfcnchnthtolhdioihdpyazmrkhyos
wmvtienngodmbnswdsmotscafxeyproycseylftpspldtpsoisfwgmhsiekojliaet
iaetdljkjkishejkiniojtinjtiohejeihkkjkoyadtpsojnflinjyfdkpidfpiaia
kktpsotanshftanehsksgdjkjkisdpihieeyececehescxfpfpfpfpfxeoglknhsfx
tpcxksdaisjyjyjojkftdldlhsjoindmioinjyiskpiddmiajljndlkpjkihjpjkdl
jtiocxjeihkkcxjpihioinjkjyihjpihiecxjljtcxflinjyfdkpidcxhsjkcxjliy
fpfpfpfpfpgyfpfpfpfygtfpfpfpfpgsiaeogljlgshghfjegtimgoehgtghjefpfp
gofpfpfpfpfpfpfpfpfpfwjtgljlhkghgaehgliofpfpfpfggtfpfpfpfpgsiaeogl
jokpgogygygsgagtksjlhkeydyeybkfgkkgteodljojoieecjnkkfehkfghgesisgd
tpsoksgdjkjkisdpihieeyececehescxfpfpfpfpfxeoglknhsfxehjzhtfygaehgl
axtpsotansghlfaohdfztsqzzmldmhgdgycwrynsbbcnmuistpiyjtldbsdatpjold
```

Our Learning XIDs course offers GitHub as a simple starting point. You can publish a XID to your GitHub, you can update it as you see fit, and you can prove control of the GitHub with registered signing keys. But it's far from a perfect solution: GitHub is already censored in some fascist regimes, and even if it's trustworthy now, we don't know that'll be the case in a year (or ten years).



XIDS & GARNER

ENTER GARNER

- Tor Endpoint for SSI
- Let's You Serve SSI Documents Including XIDs
- Private, Censorship-Resistant
- Truly Self-Sovereign
  - You Run It

or Onion Service

Overview

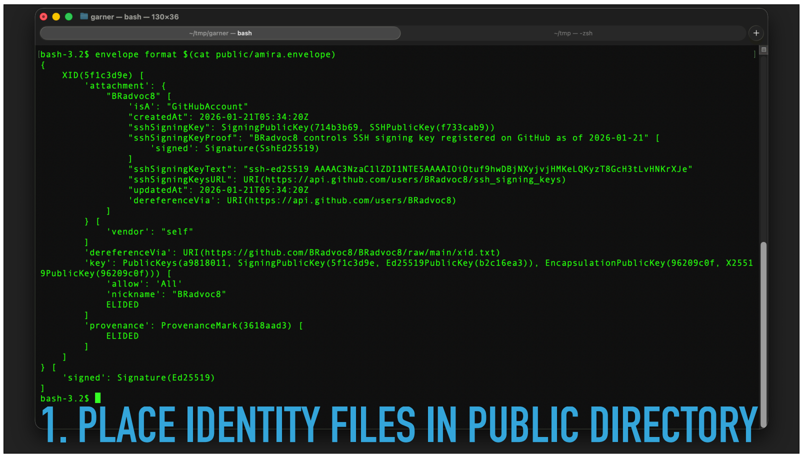
A developer tool that provides a Tor endpoint for self-sovereign identity.
HTTP to allow the retrieval of authenticated identity documents.

Why is Garner Important?

elf-sovereign identity documents. It has five major stren
use of `HTTPS` or even bare `tor`.

ty: The ultimate goal of Garner is self-sovereignty. XIDs
lentity that they can issue, hold, and redact as they see
allows them to also distribute their own identity docume

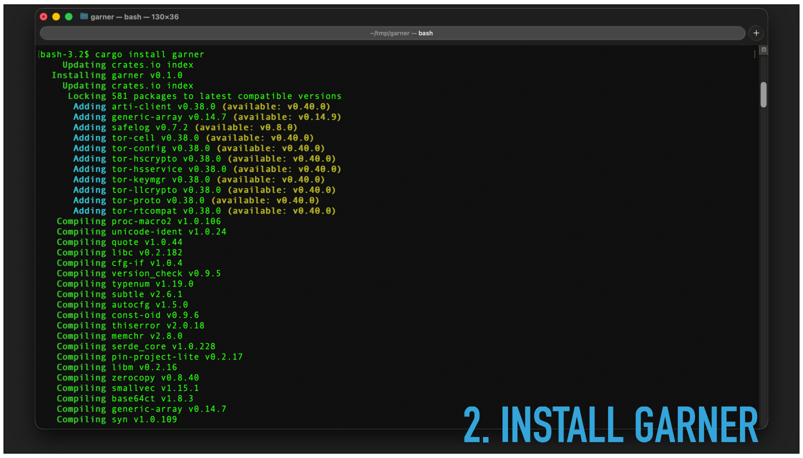
That's where our newest technology comes in: Garner, which is a Tor Onion Service specifically built for serving identity documents in a self-sovereign way. You control what's transmitted, you prove ownership with key pairs, and you can't be censored unless Tor is entirely blocked. (And if it is, Garner is just one solution we have for transmitting identity information. Take a look at our fall 2025 videos on Hubert for another option.)



```
bash-3.2$ envelope format $(cat public/amira.envelope)
{
    XID(5f1c3d9e) [
        'attachment': {
            "BRadvoc8" [
                'isA': "GitHubAccount"
                "createdAt": 2026-01-21T05:34:20Z
                "sshSigningKey": SigningPublicKey(714b3b69, SSHPublicKey(f733cab9))
                "sshSigningKeyProof": "BRadvoc8 controls SSH signing key registered on GitHub as of 2026-01-21" [
                    'signed': Signature(SshEd25519)
                ]
                "sshSigningKeyText": "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOiOtuf9hwDBjNXyjvjHMKeLQKyzT8GcH3tLvHNKrXJe"
                "sshSigningKeysURL": URI(https://api.github.com/users/BRadvoc8/ssh_signing_keys)
                "updatedAt": 2026-01-21T05:34:20Z
                'dereferenceVia': URI(https://api.github.com/users/BRadvoc8)
            ]
        } [
            'vendor': "self"
        ]
        'dereferenceVia': URI(https://github.com/BRadvoc8/BRadvoc8/raw/main/xid.txt)
        'key': PublicKeys(a9818011, SigningPublicKey(5f1c3d9e, Ed25519PublicKey(b2c16ea3)), EncapsulationPublicKey(96209c0f, X2551
9PublicKey(96209c0f))) [
            'allow': 'All'
            'nickname': "BRadvoc8"
            ELIDED
        ]
        'provenance': ProvenanceMark(3618aad3) [
            ELIDED
        ]
    ]
} [
    'signed': Signature(Ed25519)
]
bash-3.2$ 
```

1. PLACE IDENTITY FILES IN PUBLIC DIRECTORY

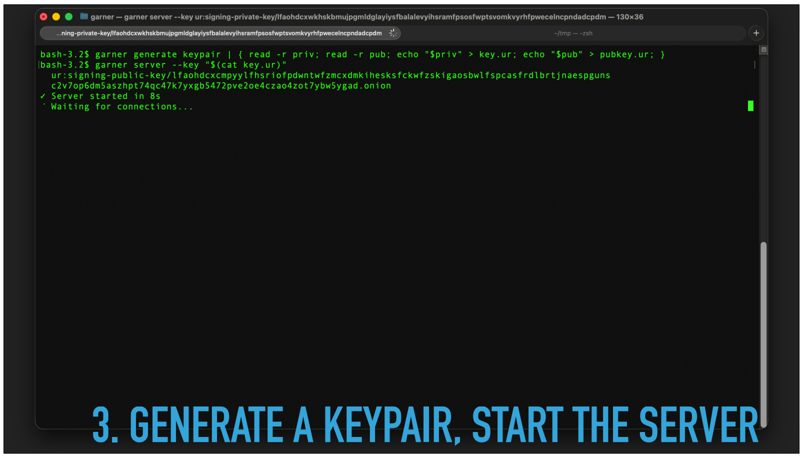
Garner is also really easy to use. One of the reasons we suggested other options like GitHub is because creating web sites is very hard for the average user. You need to buy a DNS record, you need to manage SSL certs, and that’s all before running Apache or some other complex program. For Garner, there are just a few simple steps. First, you place the files you want to publish in a “public” directory.



```
bash-3.2$ cargo install garner
    Updating crates.io index
  Installing garner v0.1.0
    Updating crates.io index
     Locking 581 packages to latest compatible versions
      Adding arti-client v0.38.0 (available: v0.40.0)
      Adding generic-array v0.14.7 (available: v0.14.9)
      Adding safelog v0.7.2 (available: v0.8.0)
      Adding tor-cell v0.38.0 (available: v0.40.0)
      Adding tor-config v0.38.0 (available: v0.40.0)
      Adding tor-hscrypto v0.38.0 (available: v0.40.0)
      Adding tor-hsservice v0.38.0 (available: v0.40.0)
      Adding tor-keymgr v0.38.0 (available: v0.40.0)
      Adding tor-llcrypto v0.38.0 (available: v0.40.0)
      Adding tor-proto v0.38.0 (available: v0.40.0)
      Adding tor-rtcompat v0.38.0 (available: v0.40.0)
   Compiling proc-macro2 v1.0.106
   Compiling unicode-ident v1.0.24
   Compiling quote v1.0.44
   Compiling libc v0.2.182
   Compiling cfg-if v1.0.4
   Compiling version_check v0.9.5
   Compiling typenum v1.19.0
   Compiling subtle v2.6.1
   Compiling autocfg v1.5.0
   Compiling const-oid v0.9.6
   Compiling thiserror v2.0.18
   Compiling memchr v2.8.0
   Compiling serde_core v1.0.228
   Compiling pin-project-lite v0.2.17
   Compiling libm v0.2.16
   Compiling zerocopy v0.8.40
   Compiling smallvec v1.15.1
   Compiling base64ct v1.8.3
   Compiling generic-array v0.14.7
   Compiling syn v1.0.109
```

2. INSTALL GARNER

Second, you install Garner, which is done through a Rust crate, which makes it an automated process.

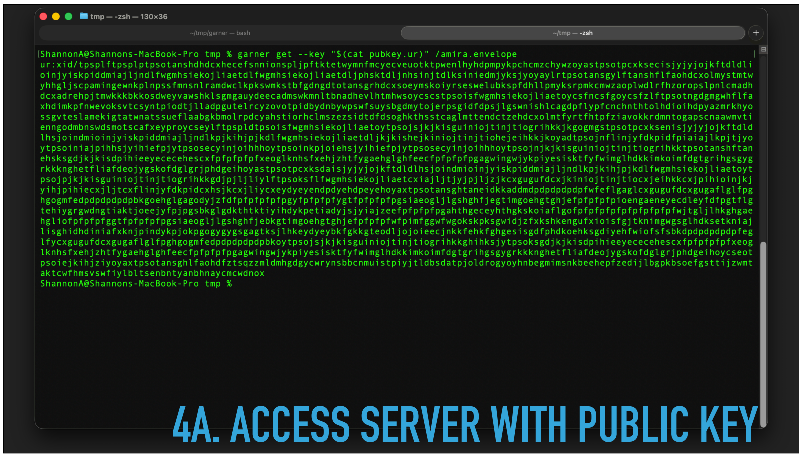


garner — garner server --key ur:signing-private-key/lfaohdcxwkhskbmujpgmldglayiysfbalalevyihsramfpsosfwptsvomkvyrhfpwecelncpndadcpdm — 130×36
...ning-private-key/lfaohdcxwkhskbmujpgmldglayiysfbalalevyihsramfpsosfwptsvomkvyrhfpwecelncpndadcpdm
~/tmp — -zsh

```
bash-3.2$ garner generate keypair | { read -r priv; read -r pub; echo "$priv" > key.ur; echo "$pub" > pubkey.ur; }
bash-3.2$ garner server --key "$(cat key.ur)"
  ur:signing-public-key/lfaohdcxcmpyylfhsriofpdwntwfzmcxdmkiheskfsfckwfzskigaosbwlfspcasfrdlbrtjnaespguns
  c2v7op6dm5aszhpt74qc47k7yxgb5472pve2oe4czao4zot7ybw5ygad.onion
✓ Server started in 8s
  Waiting for connections...
```

3. GENERATE A KEYPAIR, START THE SERVER

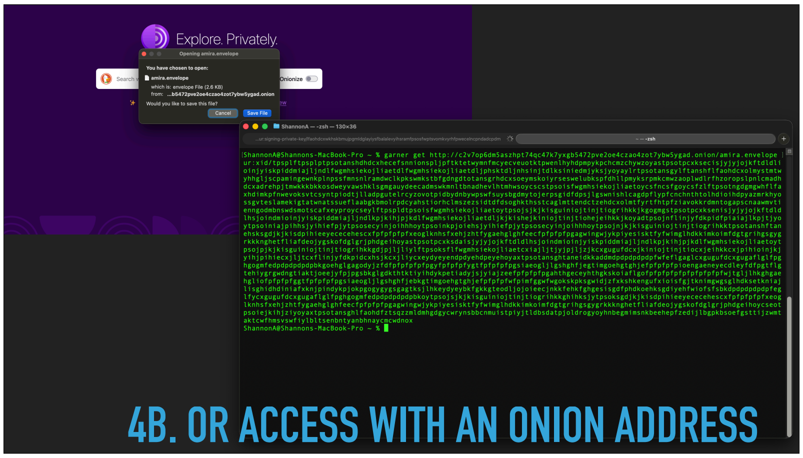
Third, you generate a key pair, something you only have to do the first time, and then you start the Garner server with your private key.



```
ShannonA@Shannons-MacBook-Pro tmp % garner get --key "$(cat pubkey.ur)" /amira.envelope
ur:xid/tpsplftpsplptpsotanshdhdcxhecefsnnionspljpftktetwymnfmcyecveuotktpwenlhyhdpmpykpchcmzchywzoyastpsotpcxksecisjyjyjojkftdldli
oinjyiskpiddmiajljndlfwgmhsiekojliaetdlfwgmhsiekojliaetdljphsktdljnhsinjtdlksiniedmjyksjyoyaylrtpsotansgylftanshflfaohdcxolmystmtw
yhhgljscpamingewnkplnpssfmnsnlramdwclkpkswmkstbfgdngdtotansgrhdcxsoeymskoiyrseswelubkspfdhllpmyksrpmkcmwzaoplwdlrfhzoropslpnlcmadh
dcxadrehpjtmwkkkbkkosdweyvawshklsgmgauydeecadmswkmnltbnadhevlhtmhwsoycscstpsoisfwgmhsiekojliaetoycsfncsfgoycsfzlftpsotngdgmgwhflfa
xhdimkpfnwevoksvtcsyntpiodtjlladpgutelrcyzovotpidbydnbywpswfsuysbgdmytojerpsgidfdpsjlgswnishlcagdpflypfcnchnthtolhdioihdpyazmrkhyo
ssgvteslamekigtatwnatssueflaabgkbmolrpdcyahstiorhclmszezsidtdfdsoghkthsstcaglmttendctzehdcxolmtfyrtfhtpfziavokkrdmntogapscnaawmvti
enngodmbnswdsmotscafxeyproycseylftpspldtpsoisfwgmhsiekojliaetoytpsojsjkjkisguiniojtinjtiogrihkkjkgogmgstpsotpcxksenisjyjyjojkftdld
lhsjoindmioinjyiskpiddmiajljndlkpjkihjpjkdlfwgmhsiekojliaetdljkjkishejkiniojtinjtiohejeihkkjkoyadtpsojnflinjyfdkpidfpiaiajlkpjtjyo
ytpsoiniajpihhsjyihiefpjytpsosecyinjoihhhoytpsoinkpjoiehsjyihiefpjytpsosecyinjoihhhoytpsojnjkjkisguiniojtinjtiogrihkktpsotanshftan
ehsksgdjkjkisdpihieeyececehescxfpfpfpfpfxeoglknhsfxehjzhtfygaehglghfeecfpfpfpfpgagwingwjykpiyesisktfyfwimglhdkkimkoimfdgtgrihgsgyg
rkkknghetfliafdeojygskofdglgrjphdgeihoyastpsotpcxksdaisjyjyjojkftdldlhsjoindmioinjyiskpiddmiajljndlkpjkihjpjkdlfwgmhsiekojliaetoyt
psojpjkjkisguiniojtinjtiogrihkkgdjpjljliylftpsoksflfwgmhsiekojliaetcxiajljtjyjpjljzjkcxgugufdcxjkiniojtinjtiocxjeihkkcxjpihioinjkj
yihjpihiecxjljtcxflinjyfdkpidcxhsjkcxjliycxeydyeyendpdyehdpeyehoyaxtpsotansghtaneidkkaddmdpdpdpdpdpfwfeflgaglcxgugufdcxgugaflglfpg
hgogmfedpdpdpdpdpbkgoehglgagodyjzfdfpfpfpfpfpgyfpfpfpfygtfpfpfpfpgsiaeogljlgshghfjegtimgoehgtghjefpfpfpfpioengaeneyecdleyfdfpgtflg
tehiygrgwdngtiaktjoeejyfpjpgsbkglgdkthtktiyihdykpetiadyjsjyiajzeefpfpfpfpgahthgeceyhthgkskoiaflgofpfpfpfpfpfpfpfpfpfwjtgljlhkghgae
hgliofpfpfpfggtfpfpfpfpgsiaeogljlgshghfjebkgtimgoehgtghjefpfpfpfwfpimfggwfwgokskpksgwidjzfxkshkengufxioisfgjtknimgwgsglhdksetkniaj
lisghidhdiniafxknjpindykpjokpgogygygsgagtksjlhkeydyeybkfgkkgteodljojoieecjnkkfehkfghgesisgdfphdkoehksgdiyehfwiofsfsbkdpdpdpdpdpfeg
lfycxgugufdcxgugaflglfpghgogmfedpdpdpdpdpbkoytpsojsjkjkisguiniojtinjtiogrihkkghihksjytpsoksgdjkjkisdpihieeyececehescxfpfpfpfpfxeog
lknhsfxehjzhtfygaehglghfeecfpfpfpfpgagwingwjykpiyesisktfyfwimglhdkkimkoimfdgtgrihgsgygrkkknghetfliafdeojygskofdglgrjphdgeihoycseot
psoiejkihjziyoyaxtpsotansghlfaohdfztsqzzmldmhgdgycwrynsbbcnmuistpiyjtldbsdatpjoldrogyoyhnbegmimsnkbeehepfzedijlbgpkbsoefgsttijzwmt
aktcwfhmsvswfiylbltsenbntyanbhnaycmcwdnox
ShannonA@Shannons-MacBook-Pro tmp %
```

4A. ACCESS SERVER WITH PUBLIC KEY

Finally, you give out the public key and the file name to other people and they can use Garner as a client to access your files. No DNS, no SSL cert, no complex Apache configuration, just a directory of files and a key pair! (An index file can make things even simpler!)



Explore. Privately.
Search
Onionize

Opening amira.envelope

You have chosen to open:

amira.envelope

which is: envelope File (2.6 KB)
from: ...b5472pve2oe4czao4zot7ybw5ygad.onion

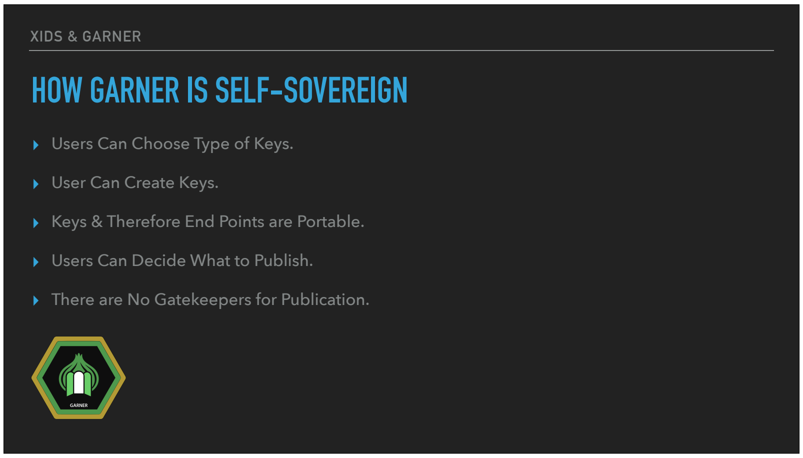
Would you like to save this file?

Cancel
Save File
ShannonA — -zsh — 130×36
...ur:signing-private-key/lfaohdcxwkhskbmujpgmldglayiysfbalalevyihsramfpsosfwptsvomkvyrhfpwecelncpndadcpdm
~ — -zsh

```
ShannonA@Shannons-MacBook-Pro ~ % garner get http://c2v7op6dm5aszhpt74qc47k7yxgb5472pve2oe4czao4zot7ybw5ygad.onion/amira.envelope
ur:xid/tpsplftpsplptpsotanshdhdcxhecefsnnionspljpftktetwymnfmcyecveuotktpwenlhyhdpmpykpchcmzchywzoyastpsotpcxksecisjyjyjojkftdldli
oinjyiskpiddmiajljndlfwgmhsiekojliaetdlfwgmhsiekojliaetdljphsktdljnhsinjtdlksiniedmjyksjyoyaylrtpsotansgylftanshflfaohdcxolmystmtw
yhhgljscpamingewnkplnpssfmnsnlramdwclkpkswmkstbfgdngdtotansgrhdcxsoeymskoiyrseswelubkspfdhllpmyksrpmkcmwzaoplwdlrfhzoropslpnlcmadh
dcxadrehpjtmwkkkbkkosdweyvawshklsgmgauydeecadmswkmnltbnadhevlhtmhwsoycscstpsoisfwgmhsiekojliaetoycsfncsfgoycsfzlftpsotngdgmgwhflfa
xhdimkpfnwevoksvtcsyntpiodtjlladpgutelrcyzovotpidbydnbywpswfsuysbgdmytojerpsgidfdpsjlgswnishlcagdpflypfcnchnthtolhdioihdpyazmrkhyo
ssgvteslamekigtatwnatssueflaabgkbmolrpdcyahstiorhclmszezsidtdfdsoghkthsstcaglmttendctzehdcxolmtfyrtfhtpfziavokkrdmntogapscnaawmvti
enngodmbnswdsmotscafxeyproycseylftpspldtpsoisfwgmhsiekojliaetoytpsojsjkjkisguiniojtinjtiogrihkkjkgogmgstpsotpcxksenisjyjyjojkftdld
lhsjoindmioinjyiskpiddmiajljndlkpjkihjpjkdlfwgmhsiekojliaetdljkjkishejkiniojtinjtiohejeihkkjkoyadtpsojnflinjyfdkpidfpiaiajlkpjtjyo
ytpsoiniajpihhsjyihiefpjytpsosecyinjoihhhoytpsoinkpjoiehsjyihiefpjytpsosecyinjoihhhoytpsojnjkjkisguiniojtinjtiogrihkktpsotanshftan
ehsksgdjkjkisdpihieeyececehescxfpfpfpfpfxeoglknhsfxehjzhtfygaehglghfeecfpfpfpfpgagwingwjykpiyesisktfyfwimglhdkkimkoimfdgtgrihgsgyg
rkkknghetfliafdeojygskofdglgrjphdgeihoyastpsotpcxksdaisjyjyjojkftdldlhsjoindmioinjyiskpiddmiajljndlkpjkihjpjkdlfwgmhsiekojliaetoyt
psojpjkjkisguiniojtinjtiogrihkkgdjpjljliylftpsoksflfwgmhsiekojliaetcxiajljtjyjpjljzjkcxgugufdcxjkiniojtinjtiocxjeihkkcxjpihioinjkj
yihjpihiecxjljtcxflinjyfdkpidcxhsjkcxjliycxeydyeyendpdyehdpeyehoyaxtpsotansghtaneidkkaddmdpdpdpdpdpfwfeflgaglcxgugufdcxgugaflglfpg
hgogmfedpdpdpdpdpbkgoehglgagodyjzfdfpfpfpfpfpgyfpfpfpfygtfpfpfpfpgsiaeogljlgshghfjegtimgoehgtghjefpfpfpfpioengaeneyecdleyfdfpgtflg
tehiygrgwdngtiaktjoeejyfpjpgsbkglgdkthtktiyihdykpetiadyjsjyiajzeefpfpfpfpgahthgeceyhthgkskoiaflgofpfpfpfpfpfpfpfpfpfwjtgljlhkghgae
hgliofpfpfpfggtfpfpfpfpgsiaeogljlgshghfjebkgtimgoehgtghjefpfpfpfwfpimfggwfwgokskpksgwidjzfxkshkengufxioisfgjtknimgwgsglhdksetkniaj
lisghidhdiniafxknjpindykpjokpgogygygsgagtksjlhkeydyeybkfgkkgteodljojoieecjnkkfehkfghgesisgdfphdkoehksgdiyehfwiofsfsbkdpdpdpdpdpfeg
lfycxgugufdcxgugaflglfpghgogmfedpdpdpdpdpbkoytpsojsjkjkisguiniojtinjtiogrihkkghihksjytpsoksgdjkjkisdpihieeyececehescxfpfpfpfpfxeog
lknhsfxehjzhtfygaehglghfeecfpfpfpfpgagwingwjykpiyesisktfyfwimglhdkkimkoimfdgtgrihgsgygrkkknghetfliafdeojygskofdglgrjphdgeihoycseot
psoiejkihjziyoyaxtpsotansghlfaohdfztsqzzmldmhgdgycwrynsbbcnmuistpiyjtldbsdatpjoldrogyoyhnbegmimsnkbeehepfzedijlbgpkbsoefgsttijzwmt
aktcwfhmsvswfiylbltsenbntyanbhnaycmcwdnox
ShannonA@Shannons-MacBook-Pro ~ %
```

4B. OR ACCESS WITH AN ONION ADDRESS

Onion addresses are also generated deterministically from the keys. The advantage of giving out keys is they can be used to prove ownership, but giving out addresses makes things simpler. Other people can use Garner with either the onion address or public key from from the command line, or even use a Tor browser to download the files.

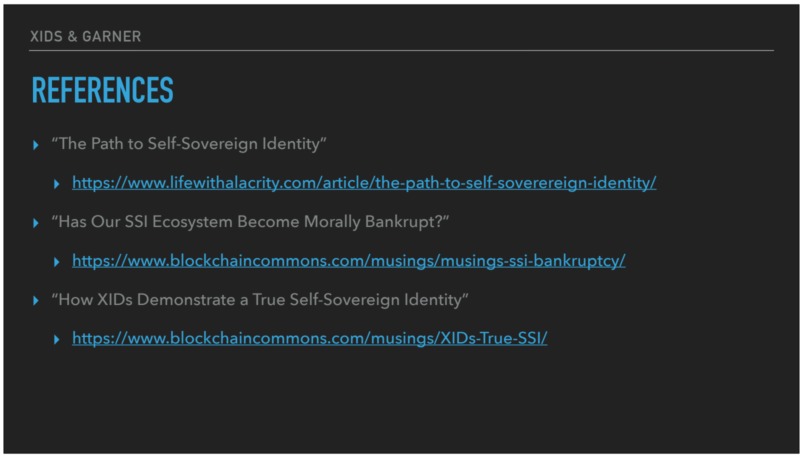


XIDS & GARNER

HOW GARNER IS SELF-SOVEREIGN

- Users Can Choose Type of Keys.
- User Can Create Keys.
- Keys & Therefore End Points are Portable.
- Users Can Decide What to Publish.
- There are No Gatekeepers for Publication.

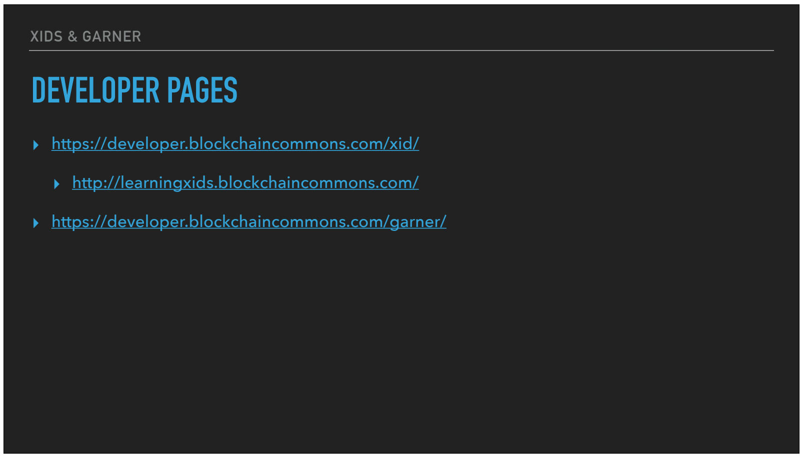
Again, we can see how the self-sovereign principles are supported. You're in control of everything. As long as you have your keys, you can start up your Garner server anywhere, and anyone who has that public key or onion address can access it. There are no gatekeepers getting in your way, and thanks to the privacy of Tor it's all censorship- and coercion-resistant. It's the next step in self-sovereign identity: self-sovereign networking to allow self-sovereign publication.



REFERENCES

- “The Path to Self-Sovereign Identity”
  - https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/
- “Has Our SSI Ecosystem Become Morally Bankrupt?“
  - https://www.blockchaincommons.com/musings/musings-ssi-bankruptcy/
- “How XIDs Demonstrate a True Self-Sovereign Identity”
  - https://www.blockchaincommons.com/musings/XIDs-True-SSI/

Here’s the trilogy of articles that define how I’ve looked at self-sovereign identity over the years: my 2016 intro to SSI and my more recent articles on how the ecosystem has failed the principles of SSI and how I think that XIDs can turn that around.

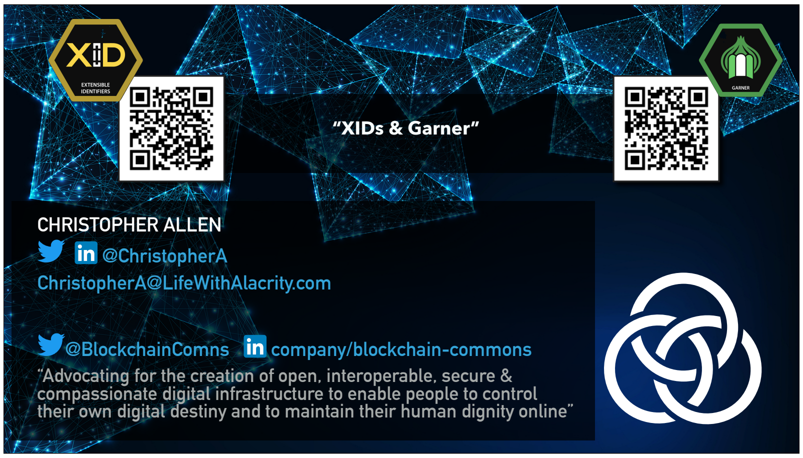


XIDS & GARNER

DEVELOPER PAGES

- https://developer.blockchaincommons.com/xid/
  - http://learningxids.blockchaincommons.com/
- https://developer.blockchaincommons.com/garner/

As usual, we’ve got more on our developer pages, including a lot of sub-links to other material related to XIDs and Garner.



“XIDs & Garner”

CHRISTOPHER ALLEN
@ChristopherA
ChristopherA@LifeWithAlacrity.com

@BlockchainComns company/blockchain-commons

“Advocating for the creation of open, interoperable, secure & compassionate digital infrastructure to enable people to control their own digital destiny and to maintain their human dignity online”

XiD
EXTENSIBLE IDENTIFIERS
GARNER

Here’s QR codes for the XID and Garner pages for more info.

I’m now happy to take questions on these technologies or to discuss some of the underlying principles and goals of self-sovereign identity, and the problems it’s facing today.