



Blockchain Commons

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



BLOCKCHAIN COMMONS

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](mailto:fda6c78e)



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.



BECOME A SPONSOR

 **Bitmark**

 **chia**

 **CROSSBAR**



 **FOUNDATION**

 **Human Rights Foundation**

 **unchained capital**

 **Zcash**
Community Grants

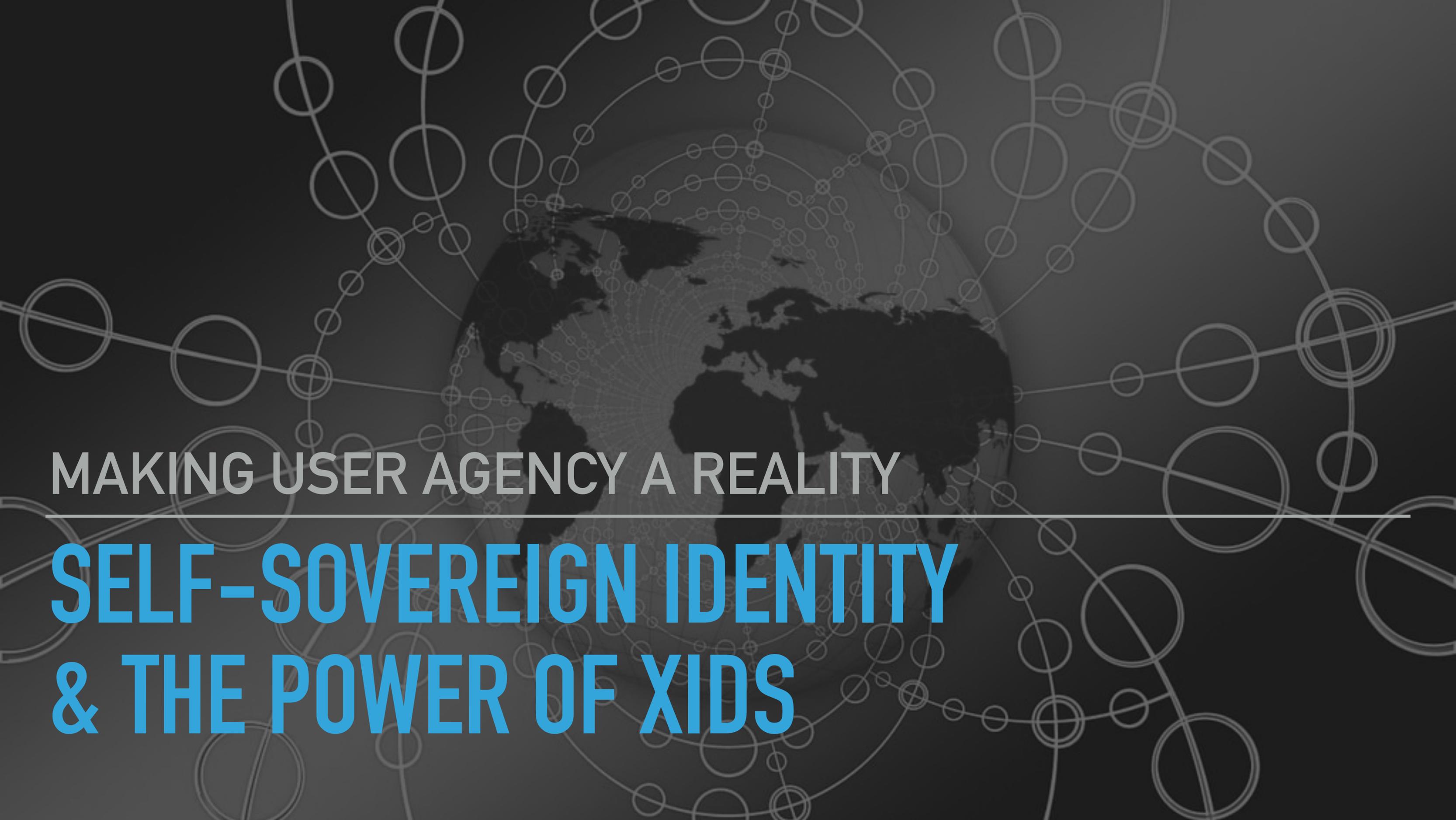




BLOCKCHAIN COMMONS

NEW TECHNOLOGY VIDEO





MAKING USER AGENCY A REALITY

SELF-SOVEREIGN IDENTITY & THE POWER OF XIDS

SELF-SOVEREIGN IDENTITY

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



10 PRINCIPLES OF SELF-SOVEREIGN IDENTITY



existence



control



access



transparency



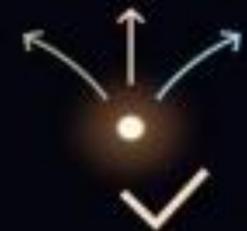
persistence



portability



interoperability



consent



minimization



protection

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!



XIDS ARE SSI DONE RIGHT

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



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 without changing the identifier. It does not necessarily to it is inspired by the same needs and desires.

Important?

One of the key features of XIDs is that they allow for the **redaction** of



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.



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

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





TRANSMITTING SSI

**FROM GITHUB
TO 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!



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



```
raw.githubusercontent.com/BRadvoc8/BRadvoc8/main/xid.txt  
  
pspltpotanshdhdcxhecefsnnionspljpfktetwymnfmcyecveuotktpwenlhyhd  
ksiniedmjyksjyoyaylrtpotansgylftanshflfaohdcxolmystmtwyhhgljscpar  
lrehpjtmmwkkkbkkosdweyvawshklsgmgauydeecadmawkmnlbnadhevltmhwsocys  
ogdmytojerpsgidfdpsjlgswnishlcagdpflypfcncnhtthldioihdpyazmrkhyos  
wvmtiennngodmbnswdsmotscafxyproycseylftpspltpsoisfwgmhsiekojliaet  
liaetdljkjkishejkiniojtinjtiohejeihkkjkoyadtpsojnflinjyfdkpidfpiaia  
kktpotanshftanehsksgdjkjkisdpihieeyececehescxpfpfpfpfxeoglnhsfx  
otpcxksdaisjyjojkftdlhsjoindmioinjyiskpidmiajljndlkpkjihjpkdl  
jtiocxjeihkkcxjpihioinjkyihjpihiecxjljtcxflinjyfdkpidcxhsjkcxjliy  
lfpfpfpfpfgyfpfpfpfygtfpfpfpfpgsiaeogljlgshghfjegtimgoehgtghjefpfp  
gofpfpfpfpfpfpfpfpfwjtgjlhkgghaehglfiofpfpfpfggtfpfpfpfpgsiaeogl  
jokpgogygygsgagtsjlhkeydyeybkfkgkgtedljojoieecjnkkfekfghgesisgd  
rtpsoksgdjkjkisdpihieeyececehescxpfpfpfpfxeoglnhsfxehjzhtfygaehgl  
rxtpsotansghlfaohdfztsqzzmlmhgdgycwrynsbbcnmuistpiyjtldbsdatpjo ld
```



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?

self-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](#) identity that they can issue, hold, and redact as they see allows them to also distribute their own identity docume



```
[bash-3.2$ envelope format $(cat public/amira.envelope)
{
  XID(5f1c3d9e) [
    'attachment': {
      "BRadvoc8" [
        'isA': "GitHubAccount"
        "createdAt": 2026-01-21T05:34:20Z
        "sshSigningKey": SigningPublicKey(714b3b69, SSHPublicKey(f733cab9))
        "sshSigningKeyProof": "BRadvoc8 controls SSH signing key registered on GitHub as of 2026-01-21" [
          'signed': Signature(SshEd25519)
        ]
        "sshSigningKeyText": "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAI0i0tuf9hwDBjNXyvjHMKeLQKyzT8GcH3tLvHNKrXJe"
        "sshSigningKeysURL": URI(https://api.github.com/users/BRadvoc8/ssh_signing_keys)
        "updatedAt": 2026-01-21T05:34:20Z
        'dereferenceVia': URI(https://api.github.com/users/BRadvoc8)
      ]
    } [
      'vendor': "self"
    ]
    'dereferenceVia': URI(https://github.com/BRadvoc8/BRadvoc8/raw/main/xid.txt)
    'key': PublicKeys(a9818011, SigningPublicKey(5f1c3d9e, Ed25519PublicKey(b2c16ea3)), EncapsulationPublicKey(96209c0f, X25519PublicKey(96209c0f))) [
      'allow': 'All'
      'nickname': "BRadvoc8"
      ELIDED
    ]
    'provenance': ProvenanceMark(3618aad3) [
      ELIDED
    ]
  ]
} [
  'signed': Signature(Ed25519)
]
bash-3.2$ █
```

1. PLACE IDENTITY FILES IN 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

```
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/lfaohdcxcmpyylfhsrioofdwntwfmzcxdkihesksfckwfzskigaosbwlfspcasfrdlbrtjnaespguns
  c2v7op6dm5aszhpt74qc47k7yxgb5472pve2oe4czao4zot7ybw5ygad.onion
✓ Server started in 8s
` Waiting for connections...
```

3. GENERATE A KEYPAIR, START THE SERVER

```

[ShannonA@Shannons-MacBook-Pro tmp % garner get --key "$(cat pubkey.ur)" /amira.envelope
ur:xid/tpsplftpspltpstanshdhdcxhecefsnnionspljpfktetwymnfmcyecveuotktpwenlhyhdpmypkpchcmzchyzoyastpsotpcxksecisjyjojkftdldli
oinjyiskpidmiaajljndlfwgmhsiekoljiaetdlfwgmhsiekoljiaetdljphsktdljnhsinjtdlksiniedmjyksjyoyaylrtpotansgylftanshflfaohdcxolmystmtw
yhhgljscpamingewnkplnpsfmsnlramdwclpkswmkstbfgdngdtotansgrhdcxsoeyskoiyrsewelubkspfdhllpmyksrpmkcmwzaoplwdlrfhzoropslnlcmadh
dcxadrehpjtwwkkkkkosdweyvawshklsgmgauydeecadmswkmnltnadhevltmhwsyoyscscstpsoisfwgmhsiekoljiaetoysfncsfgoysfzlfpsotngdgmghflfa
xhdimkpfnwvoksvtcsyntpiodtjlladpgutelrcyzovotpidbydnbywpswfsuysbgdmytojerpsgidfdpsjlgswnishlcagdpflypfcncnhtthldioihdpyazmrkhyo
ssgvteslamekigtatwnatssueflaabgkblmrlpdcyahstiorhclmszezsiddfdsoghkthsstcaglmittendctzehdcxolmtfyrftfhtpfziaavokkrdmntogapscnaawmti
enngodmbnswdsmotscafxyproycseylftpspldtpsoisfwgmhsiekoljiaetoypsojsjkjkisguiniojtinjtioagrihkkjkogmgstpsotpcxksenisjyjojkftdld
lhsjoindmioinjyiskpidmiaajljndlkpkjihjpkdlfwgmhsiekoljiaetdljkjkishejkiniojtinjtiohejeihkkjkoyadtpsojnflinjyfdkpidfpiaiajlkpjtyo
ytpsoiniaajpihhsjyihiefpjtptsosecyinjoihhoytpsoinkpjoiehsjyihiefpjtptsosecyinjoihhoytpsojnjkjkisguiniojtinjtioagrihkktpotanshftan
ehsksgdjkkisdpihieeyececehesxcxfpfpfpfxeoglnhsfxehjzhtfygaehglghfeecfpfpfpfgagwingwjkpiyesisktfyfwmglhdkkimkoimfdgtgrihgsgyg
rkknghetfliafdeojygskofdglgrjphdgeihoyastpsotpcxksdaisjyjojkftdldlhsjoindmioinjyiskpidmiaajljndlkpkjihjpkdlfwgmhsiekoljiaetoyp
sojpkjkisguiniojtinjtioagrihkkgdjpljliylftpsoksflfwgmhsiekoljiaetcxiaajljtjyjpjlzjkcxgugufdcxjkiniojtinjtioecxjeihkkcxjpihioinjky
yihjpihiecxjljtcxflinjyfdkpidcxhsjkcxjliycxydyeyendpdyehdpeyehoyaxtpotansghtaneidkkaddmdpdpdpdpfweflglaglcxgugufdcxgugafglfpg
hgogmfedpdpdpdpbkgoehglgagodyjzfdfpfpfpfpfyfypfpfpfygtfpfpfpfpgsiaeogljlshghfjegtimgoehgtghjefpfpfpfpioengaeneyecdleyfdpftflg
tehiygrgdngtiaktjoeeyfjpsbkgldkthtktiyihdykpetiadyjsjyiajzeefpfpfpfgahthgeceyhthgkskoi aflgofpfpfpfpfpfpfpfpfwjtglljhkghgae
hglio ffpfpfggtfpfpfpfpgsiaeogljlshghfjebkgtimgoehgtghjefpfpfpfwfpimfggwfwgokskpkswidjzfxkshkengufxioisfgjtkningwgsglhdksetkniaj
lisghidhdiniafxknjpindykpjokpgogygygsgagtksjlhkeydyeybkfgkkgteodljojoieecjnkkfekfghgesisgdfphdkoehksgdiyehfwiofsfbkdpdpdpdpfeg
lfycxgugufdcxgugafglfpghgogmfedpdpdpdpbkoytpsojsjkjkisguiniojtinjtioagrihkkghihksjytpsoksgdjkjkisdpihieeyececehesxcxfpfpfpfxeog
lnhsfxehjzhtfygaehglghfeecfpfpfpfgagwingwjkpiyesisktfyfwmglhdkkimkoimfdgtgrihgsgygrkknghetfliafdeojygskofdglgrjphdgeihoycseot
psoiejkihjziyoyaxtpotansghlfaohdfztsqzzmlmhdggycwrynsbbcnmuistpiyjtldbsdatpjoldrogyoyhnbegmimsnkbeehepfzedijlbgpkbsoefgsttijzwm
aktcwfhmvswwfiylblttsenbntyabhnaycmwdnox
ShannonA@Shannons-MacBook-Pro tmp %

```

4A. ACCESS SERVER WITH PUBLIC KEY

Explore. Privately.



Search v

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

Onionize

```
ShannonA -- -zsh -- 130x36
...ur:signing-private-key/lfaohdcxwkhskbmujpgmldglayisfbalalevyihsrampfosfwptsvomkvyrhfpwecelncpdadcpdm ~ -zsh
[ShannonA@Shannons-MacBook-Pro ~ % garner get http://c2v7op6dm5aszhpt74qc47k7yxgb5472pve2oe4czao4zot7ybw5ygad.onion/amira.envelope ]
ur:xid/tpsplftpsplptpsotanshdhdcxhecefsnnionspljpfktetwymnfmcyecveuotktpwenlhyhdmpykpchcmzchyzoyastpsotpcxksecisjyjojkftdldli
oinjyiskpiddmiajljndlfwgmsiekojliaetdlfwgmhsiekojliaetdljphsktdljnhsinjtdlksiniedmjksjyoyaylrtpotansgylftanshflfaohdcxolmystmtw
yhhgljscpamingewnkplnpssfmnsnlramdwc lkpkswmkstbfgdngdtotansgrhdcxsoeyskoiyrsewelubkspfdhllpmyksrpmkcmwzaoplwdlrfhzoropslnlcmadh
dcxadrehpjtmwkkkbbkksdweyvawshklsgmgauydeecadmswkmnltnadhev lthmhwsoycscstpsoisfwgmhsiekojliaetoyscfncsfgoyscfzlfztpotngdgmghflfa
xhdimkpfnwsvtcsyntpiodtjlladpgutelrcyzovotpidbydnbywpswfsuysbgdmytojerpsgidfdpsjlgswnishlcagdpflypfcnchnthtolhdioihdpazmrkhyo
ssgvteslamekigtatwnatssueflaabgkblmrlpdcyahstiorhclmszezs idtdfdsoghkthsstcaglmttendctzehdcxolmtfyrthfhtpfziaavokkrdmntogapsnaawmvti
engodmbnswdmsotscafxyeproycseylftpspldtpsoisfwgmhsiekojliaetoypsojsjkjkisguiniojtinjtiohhejehkkjkoyadtpsojnflinjfdkpidfpiaiajlkpjtyo
ytpsoiniajpjihhsjyihiefpjytpsosecyinjoihhoytpsoinkpjoiehsjyihiefpjytpsosecyinjoihhoytpsojnjkjkisguiniojtinjtiohhejehkkktpotanshftan
ehsksgdjkjkisdpihieeyececehescxfpfpfpfpfxeoglnhsfxehjzhtfygaehglghfeecfpfpfpfpagawingwykpiyesisktfyfwiwglhdkkimkoimfdgtgrihsgyg
rkkknghetfliafdeojygskofdglgrjphdgeihoyastpsotpcxksdaisjyjojkftdldlshjoindmioinjyiskpiddmiajljndlkpkjihjpkdlfwgmhsiekojliaetoyp
sojppjkjkisguiniojtinjtiohhejehkkgdjppjlljlylftpsoksflfwgmhsiekojliaetcxiajljtjyppjllzjkcxgugufdcxjkiniojtinjtiohhejehkkcxjpihioinj
yihjpihiecxjljtcxflinjyfdkpidcxhsjkcxjliycxydyendpdyehdpeyehoyaxtpotansghtaneidkkaddmpdpdpdpdpfweflglaglcxgugufdcxgugafglfpg
hgogmfedpdpdpdpbkgoehglgagodyjzfdpfpfpfpfpfyfppfpfygtfppfpfpfpgsiaeogljlgshghfjegtimgoehgtghjefppfpfpfpimfggfwgokskpkswidjzfxkshkengufxioisfgjtknimgwsglhdksktniaj
lisghidhdiniafxknjpindykpkjokpgogygygsgagtkslhkeydyeybkfkgkgtedljojoieecjnkfkfghgesisgdfphdkoehksgdiyehfwiofsfsbkdpdpdpdpfeg
lfycxgugufdcxgugafglfpghgogmfedpdpdpdpbkoytpsojsjkjkisguiniojtinjtiohhejehkkghihksjytpsojsgdjkjkisdpihieeyececehescxfpfpfpfpfxeog
lnhsfxehjzhtfygaehglghfeecfpfpfpfpagawingwykpiyesisktfyfwiwglhdkkimkoimfdgtgrihsgygrkkknghetfliafdeojygskofdglgrjphdgeihoycseot
psiejkihjziyoyaxtpotansghlfaohdfztsqzzmlmhdgycwrynsbbcnmuistpijytlbdsatpjoldrogyoyhnbegmimsnkbeehepfzedijlbgpkbsoefgsttijzwm
aktcwfhmssvswfiylbltsenbntyabhnaycmwdnox
ShannonA@Shannons-MacBook-Pro ~ % █
```

4B. OR ACCESS WITH AN ONION ADDRESS

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.



REFERENCES

- ▶ “The Path to Self-Sovereign Identity”
 - ▶ <https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-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/>

DEVELOPER PAGES

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



"XIDs & Garner"

CHRISTOPHER ALLEN

  @ChristopherA

ChristopherA@LifeWithAlacrity.com

 @BlockchainComms  [company/blockchain-commons](https://www.linkedin.com/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"

