



*Questions and Answers for IIW spring 2021 about*

# KERI Q&A

## basic introduction

---

By: Henk van Cann  
[LinkedIN](#)

My objective: Personalize your own access to KERI information sources

How: I'll show you around, connect you to the Q&A, how to use it and give answers to first 10 Q's

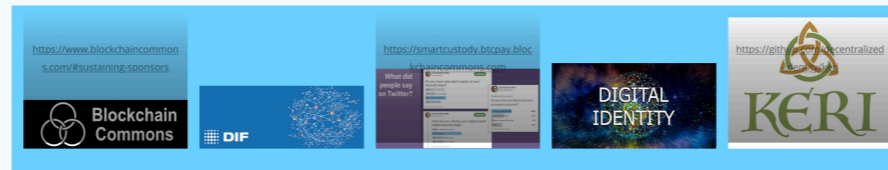
## Our spending of available funds on third-party projects

Blockchainbird sponsors meaningful projects (see [Github repo](#) for more info).

2019 : <https://smartcustody.btcpay.blockchaincommons.com>

2020 : Blockchaincommons.com general patronage DIF project KERI basic sponsoring of initiator of the project Blockchaincommons.com Torgap project

2021 : DIF project KERI?



## Contributions to third-party projects

Apart from donations in money, we would always contribute work to stay closely involved. Our ultimate goal is to become an integral part of developments that make a better world.

See [Github repo](#) for more info on what we are specifically doing for third party project involved.

*Henk van Cann*

[blockchainbird.org](https://blockchainbird.org)

[Fully Noded Q&A](#)  
[Gordian Server Q&A](#)  
[KERI Q&A](#)  
[ION Q&A](#)  
[Sidetree Q&A](#)

---

# What is KERI?

---

- ❖ Key Event Receipt Infrastructure \*\*
- ❖ Intends to *repair* the Internet \*
- ❖ KERI = CT with decentralized CA \*\*\*
- ❖ NOT a coin, token... \*

CT = Certificate Transparency and CA = Certification Authority

---

# Why KERI? (and not something else)

---

- ❖ Strong autonomous identifiers
- ❖ Abiding to privacy (laws and good habits)
- ❖ **Portability**, delegation, rotatable keys
- ❖ Direct & Indirect method
- ❖ <there's more>



# For who is KERI?

*Personalize your own access to KERI information sources*

KERI.ONE

Github KERI

Novices  
SSI advanced and proficient

Developers  
SSI Experts

Both target groups can mix the resources

# KERI.ONE



## Truly Decentralized Identity

**KERI** is the first truly decentralized identity system. It is ledger-less which means it doesn't need to use a ledger at all or ledger-portable which means that its identifiers are not locked to any given ledger and may switch as needed. In other words KERI identifiers are truly portable.



## Supports GDPR Compliance

**KERI** is inherently supportive of GDPR (global data protection rights) compliance. KERI provides non-intertwined identifier trust bases which means that a given identifier's data may be erased and truly forgotten.



## Self-Certifying Identifiers

**KERI** has a decentralized secure root-of-trust based on cryptographic self-certifying identifiers. It uses hash chained data structures called Key Event Logs that enable ambient cryptographic verifiability. In other words, any log may be verified anywhere at anytime by anybody. It has separable control over shared data which means each entity is truly self-sovereign over their identifiers.



## Scalability

**KERI** is designed for high performance and scalability. It is compatible with data intensive event streaming and event sourcing applications.



## Key Management Infrastructure

One useful way of describing **KERI** is that it is a decentralized key management infrastructure based on key change events that supports both attestable key events and consensus based verification of key events.

Features vs. OMG

Keri.one is a site, browse through it and bookmark your preferred links

# By who is KERI?

*Decentralised Identity Foundation Workgroup*

---

## Samuel M. Smith

---

Creator



Of course many other contributors, see GitHub for information.

---

# When can I use KERI?

---

- ❖ Today to study and contribute
- ❖ Today to implement the concept elsewhere
- ❖ Roadmap (current) maybe discussed in other KERI sessions



---

# How to approach KERI?

---

## Four interesting concepts to get your head around:

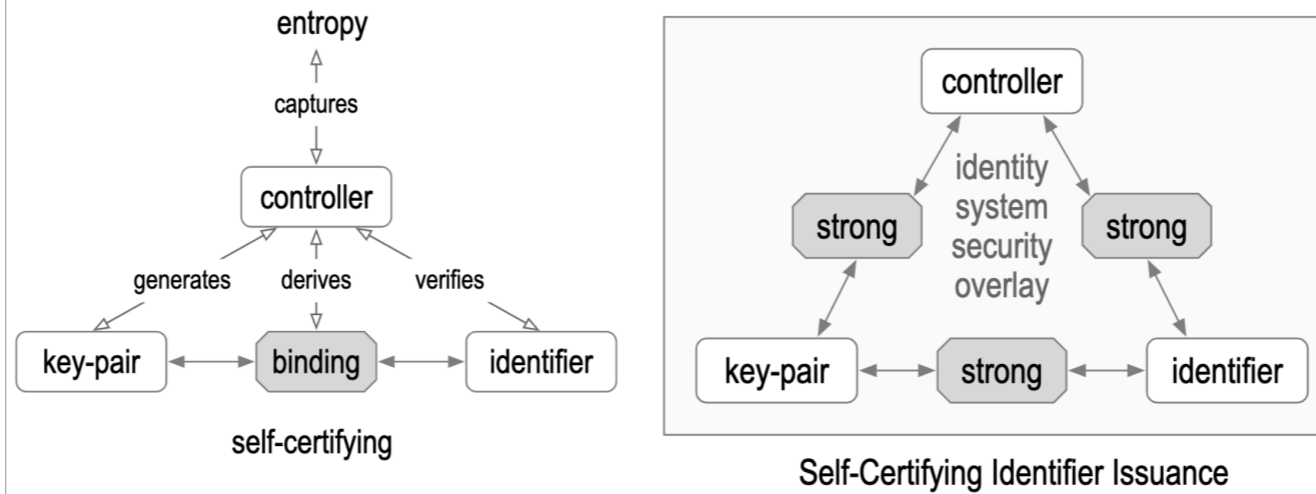
- ❖ KERI does not need a blockchain
- ❖ Duplicity detection in KERI ( public identifiers )
- ❖ Direct and indirect verification method
- ❖ Pre-rotation in KERI

This is my personal view.

What is all this ? Pre-rotation etc? Please hold your horses and use the resources offered here to find out.

# Inception of key pair of Identifier

## Self-Certifying Identifier Issuance and Binding



"Don't say KERI can't do it"

**CONTROLLER:** The entity that has the ability to make changes to an identity, cryptocurrency or verifiable credential.

The controller of an autonomous identifier is the entity (person, organization, or autonomous software) that has the capability, as defined by derivation, to make changes to an Event Log.

# What does the Q&A look like?

The screenshot shows a GitHub repository page for 'decentralized-identity / keri'. The repository is on the 'master' branch, and the current file is 'keri / docs / Q-and-A.md'. A pull request is being merged by user 'pfeairheller' from 'henkvancann/master'. The pull request has 4 contributors. The file statistics show 644 lines (491 sloc) and 48.2 KB. The document content is titled 'Q&A about KERI' and includes a 'Collaborate on HackMD' button and the KERI logo.

decentralized-identity / keri

<> Code Issues 8 Pull requests Actions Projects 1 Wiki Security Insights

master keri / docs / Q-and-A.md


pfeairheller Merge pull request #127 from henkvancann/master ✓

4 contributors

644 lines (491 sloc) 48.2 KB

## Q&A about KERI

Collaborate on HackMD



# How to use GitHub Q&A?

- ❖ [Glossary](#), [Q&A](#) and [Q&A security](#)
- ❖ User levels: \* novice, \*\* advanced, \*\*\* expert
- ❖ [Jump table to Categories](#)
- ❖ (*SamMSmith*)
- ❖ {TBW prio ...} to be written: work in progress

## Jump table to categories

### PART ONE

- [General](#)
- [Why the internet is broken](#)
- [KERI and DIDs](#)
- [Wallets](#)
- [Signatures](#)
- [Proofs](#)
- [Private Key Management](#)
- [Blockchain](#)
- [Root of trust](#)
- [KERI operational](#)
- [Agencies](#)
- [Virtual Credentials](#)

### PART TWO

- [KERI operational security](#)
- [Identifiers](#)
- [Event logs](#)
- [Inconsistency and duplicity](#)
- [Key rotation](#)
- [KEL and KELR](#)
- [Witness](#)
- [Watchers](#)
- [KERI and blockchain settled DIDs](#)
- [Security Guarantees](#)

If you get lost, try the [definitions](#) below.

What else helps better than to image you have to convince your imaginary *mother-in-law* of the usefulness of KERI?



You can read this "KERI MADE EASY" as a conversation top down



Who is Carry? Are you messing around?



KERI. Key Event Receipt Infrastructure. Not something to mess around with.

*Bonus*

Explain KERI  
to mother-in-law

[Link to page](#)

Does anyone relate to these family meetings where you have to explain to your relatives what (for heaven's sake) you are doing?



*Bonus*

**KERI security  
guarantees**

[Link to page](#)

A sincere effort to put complex language in everyday's language.

---

# 10 answers to basic questions

---

- ❖ 1-5 : What, Why, Who, When, Which way
- ❖ 6: What problem does KERI solve? \*
- ❖ 7: Who is KERI? \*
- ❖ 8: What does KERI look like? \*
- ❖ 9: What is pre-rotation? \*\*
- ❖ 10: What does KERI proof? \*