ACDC for Muggles

IIW #34
Day 1 - Session #4
26 April 2022

https://keri.one

The DAILY PROPHET
THE WIZARD WORLD'S BEGUILING BROADSHEET OF CHOICE
INCLUDED IN TODAY'S ISSUE: YOUR FREE MUGGLE JARGON-BUSTER
Today's Weather
Zodiac Aspects
Rita Skeeter's Best August Activities Corner
WIZARDING WORLD OPEN TO MUGGLES
CLAIM YOUR FREE BUTTERBEER AT THE THREE BROOMSTICKS
VOUCHER ON PAGE 11
THE MAGICAL QUILL USED TO SELECT WORTHY MUGGLES
READ MORE ABOUT POTTERMORE ON PAGES TWO, THREE AND FOUR
ROWLING CELEBRATES A HISTORIC VICTORY
MINISTRY OF MAGIC PASSES ROWLING'S PROPOSAL TO FURTHER WIZARD-MUGGLE RELATIONS
cover story continues 2
GRINGOTTS STRIKE CONTINUES 5
find the best deals in DIAGON ALLEY 7
other NEWS 9

ACDC (Authentic Chained Data Containers) is a task force of the Technology Stack Working Group at the ToIP Foundation chaired by Sam Smith.

https://trustoverip.org/

ACDC credentials are a new branch of the verifiable credentials family with special features for linking credentials together and improving speed, size, security, and privacy.

Although the full technical spec is extensive, most of the basic ideas are relatively straightforward.

The purpose of this session to explain the basic features to anyone who wants a quick high-level understanding of ACDC creds.

Format

- First, a little background from Sam
- Then 6 minutes for each of the 7 main features
    - A quick explanation of the basic idea
    - Questions for Sam—but only about that feature
    - STRICT CUT-OFF AT SIX MINUTES
- Close with a general Q&A

Meet ACDC chair Dr. Sam Smith

Note: ACDC is based on KERI—so you get KERI features for free

See the companion slide deck: **KERI for Muggles**:

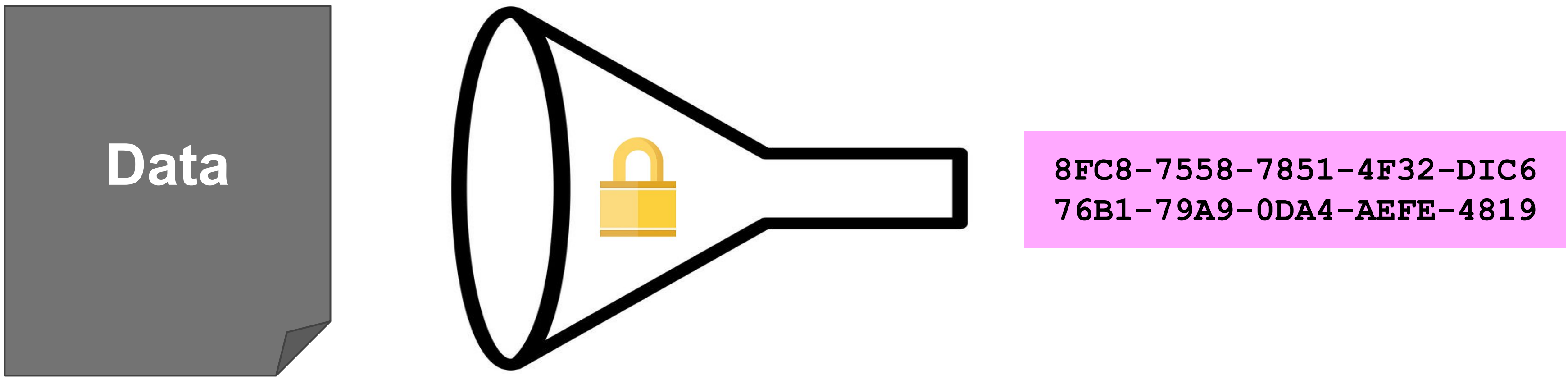
- https://keri.one/ - look for it under “Resources”
- Or go straight to it: https://docs.google.com/presentation/d/1lpzYcPrIox9V4hERtn4Kcf7uq01OVU9u3PuVm1aYzR0/edit?usp=sharing

ACDC in Seven Easy Steps

The DAILY PROPHET
THE WIZARD WORLD'S BEGUILING BROADSHEET OF CHOICE
INCLUDED IN TODAY'S ISSUE: YOUR FREE MUGGLE JARGON-BUSTER
Today's Weather
Zodiac Aspects
Rita Skeeter's Best August Activities Corner page 10
WIZARDING WORLD OPEN TO MUGGLES
CLAIM YOUR FREE BUTTERBEER AT THE THREE BROOMSTICKS
VOUCHER ON PAGE 11
READ MORE ABOUT POTTERMORE ON PAGES TWO, THREE AND FOUR
THE MAGICAL QUILL USED TO SELECT WORTHY MUGGLES
ROWLING CELEBRATES A HISTORIC VICTORY
MINISTRY OF MAGIC PASSES ROWLING'S PROPOSAL TO FURTHER WIZARD-MUGGLE RELATIONS
cover story continues 2
GRINGOTTS STRIKE CONTINUES 5
find the best deals in DIAGON ALLEY 7
other NEWS 9

First, a word from our sponsor:
cryptographic digests

All of ACDC depends on one fundamental concept: **cryptographic digests**



```
8FC8-7558-7851-4F32-DIC6
76B1-79A9-0DA4-AEFE-4819
```

Input = digital content of any kind or size

Apply cryptographic digest algorithm

Output = short, globally-unique identifier of the content

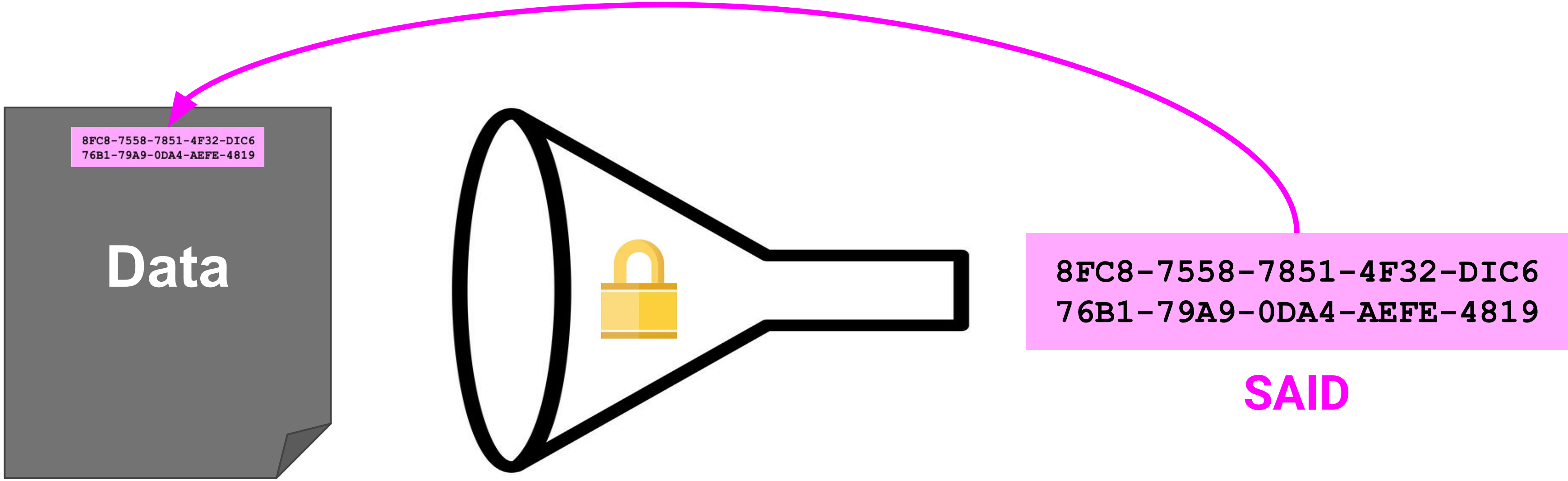
Three key features of a cryptographic digest

1. **Tamper-evident**—you can tell if even a single bit of the input data does not match the digest
2. **Can be digitally signed**—A signature on the digest has the same effect as a signature on the input data
3. **Can be privacy-preserving**—Carefully done, a digest can hide the input data until it actually needs to be shared

#1: Self-Addressing Identifiers (SAIDs)

A self-addressing identifier (SAID) is a digest that uniquely identifies content *that includes the SAID*

A SAID is a cryptographic digest *bound to its content*



Input = digital content that will include the SAID *after* hashing

Apply cryptographic digest algorithm

Output = short, globally-unique identifier of the content

NSFM (Not safe for Muggles!)

Features of SAIDs

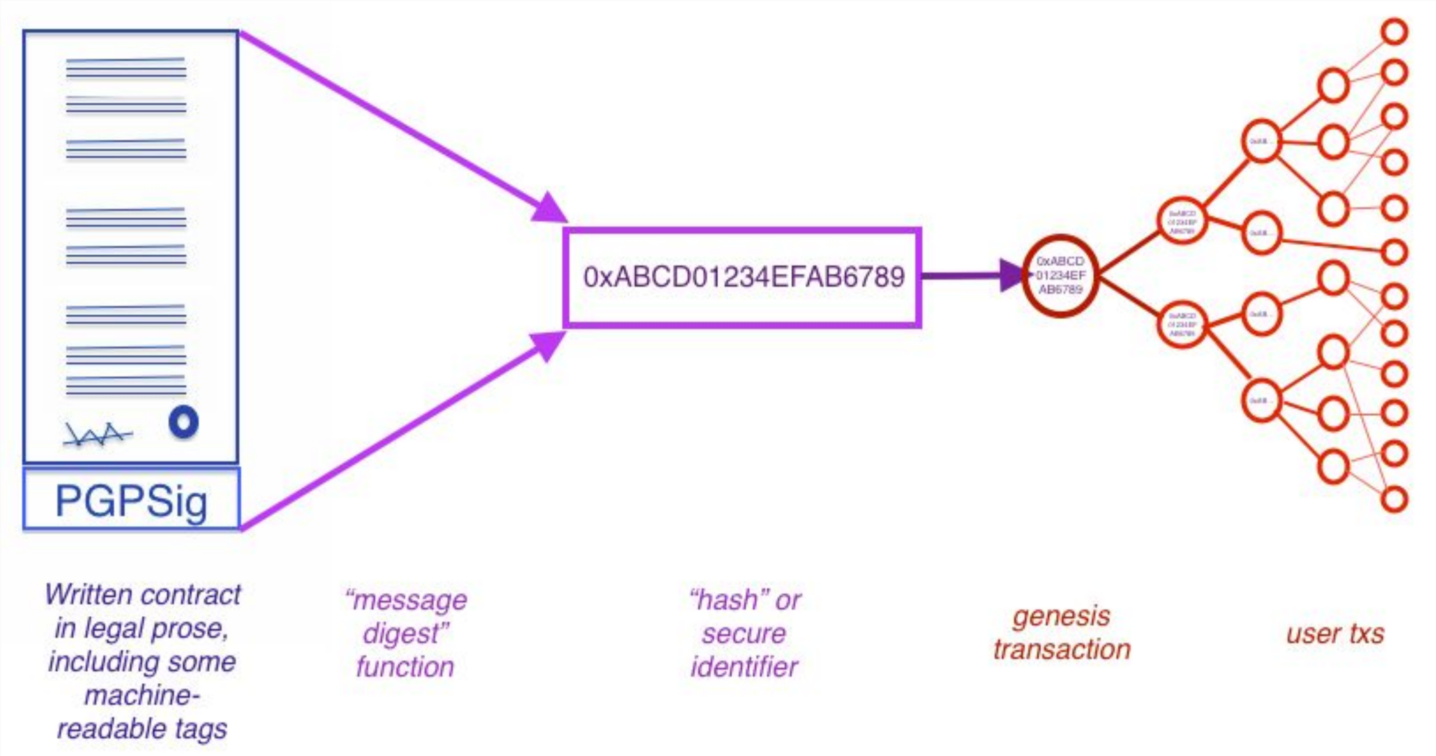
1. Because they are self-referential, there is no ambiguity about what content-addressable identifier belongs to a given block of content because the identifier is in the block.
2. You can reason globally about that block of content because the SAID is globally unique, self-referential, and cryptographically bound to that block.
3. A SAID is cryptographically agile, i.e., the SAID digest algorithm can evolve with cryptographic best practices.
4. Due to these properties, you can compress data into SAIDs so you can reason about the data without needing to send the data every time.

The Bowtie Model

World of Law

World of Cryptography

World of Accountancy


PGPSig
0xABCD01234EFAB6789
0xABCD
01234EF
AB6789
Written contract in legal prose, including some machine-readable tags
"message digest" function
"hash" or secure identifier
genesis transaction
user txs

Source: https://en.wikipedia.org/wiki/Ricardian_contract License: CC-By-SA 4.0

Benefit #1

SAIDs enable very small, efficient, secure credentials that can be easily linked together

#2: SAIDs for schemas

In ACDC, the schema(s) for a credential also have SAIDs so that the semantic structure of the credential is securely bound to it.

```
{
  "$id": "E46jrVPTzlSkUPqGGeIZ8a8FWS7a6s4reAXRZOkogZ2A",
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "title": "Public ACDC",
  "description": "Example JSON Schema Public ACDC.",
  "credentialType": "PublicACDCExample",
  "type": "object",
  "required": ["v", "d", "i", "ri", "s", "a", "e", "r"],
  "properties":  {
    "v": {
      "description": "ACDC version string",
      "type": "string"
    },
    "d": {
     "description": "ACDC SAID",
      "type": "string"
    },
    "i": {
      "description": "Issuer AID",
      "type": "string"
    },
    …
```

NSFM (Not safe for Muggles!)

Properties of immutable schema

1. Protects against schema revocation and schema malleability attacks.
2. Enables global reasoning about ACDC credential types.
3. Enables trusted registries and ecosystem governance over ACDC types.
4. Enables secure interoperable semantics.

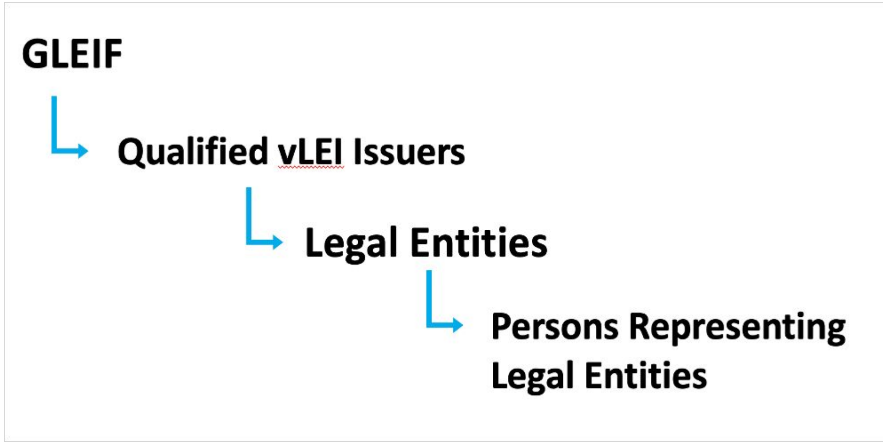
Benefit #2

Securely binding immutable schema to a credential makes it easier to define and govern different types of credentials within an ecosystem.

#3: Credential chaining

ACDC makes it very easy to chain together a set of credentials so you can verify how each credential is securely linked to the one before it.

Simple Chain



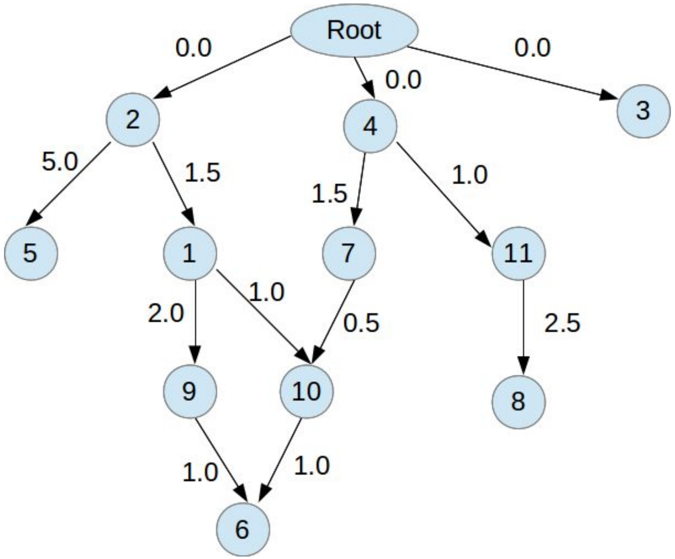
GLEIF

Qualified vLEI Issuers

Legal Entities

Persons Representing Legal Entities

Complex Chain



NSFM (Not safe for Muggles!)

Features of chaining

1. Chaining (linking) through property graphs (PGs) enables easy, powerful reasoning about provenance. PG edges have properties. “Thar’s real meat in them links!”
2. Verifiable combinatoric logic in the edges (links) enables more interoperable secure validation.
3. Verifiable delegation of authority.

Benefit #3

Chained credentials allow anyone to create secure, authentic, interoperable data supply chains

#4: Graduated disclosure

With ACDC, the holder of a credential can gradually reveal more information *about the credential itself*, not just about the data contained in the credential.

For example, in an Comprehensive Learner Record (CLR), an holder could first reveal to a verifier what kind of tests the holder has taken.

Only when the holder knows which tests are relevant would the holder reveal actual test scores.

```
"a": {
      "description": "attribute section",
      "oneOf":[
        {
          "description": "attribute section SAID",
          "type": "string"
        },
        {
          "description": "attribute detail",
          "type": "object",
          "properties": {
            "d": {
              "description": "attribute section SAID",
              "type": "string"
            },
            "i": {
              "description": "Issuee AID",
              "type": "string"
            },
            "score": {
              "description": "test score",
              "type": "integer"
            },
            "name": {
              "description": "test taker full name",
              "type": "string"
            }
          },
          "additionalProperties": false,
        }
      ]
    }
```

```
{
  "v":  "ACDC10JSON00011c_",
  "d":  "EBdXt3gIXOf2BBWNHdSXCJnFJL5OuQPyM5K0neuniccM",
  "i":  "did:keri:EmkPreYpZfFk66jpf3uFv7vklXKhzBrAqjsKAn2EDIPM",
  "ri": "did:keri:EymRy7xMwsxUelUauaXtMxTfPAMPAI6FkekwlOjkggt",
  "s":  "E46jrVPTzlSkUPqGGeIZ8a8FWS7a6s4reAXRZOkogZ2A",
  "a":  "EgveY4-9XgOcLxUderzwLIr9Bf7V_NHwY1lkFrn9y2PY",
  "e":  "ERH3dCdoFOLe71iheqcywJcnjtJtQIYPvAu6DZIl3MOA",
  "r":  "Ee71iheqcywJcnjtJtQIYPvAu6DZIl3MORH3dCdoFOLB"
}
```

NSFM (Not safe for Muggles!)

Features of Graduated Disclosure

1. Enhanced privacy protection via optional disclosure, selective disclosure, and contractually protected disclosure.
2. Enhanced performance via hierarchical caching and using SAIDs to reference credential elements.

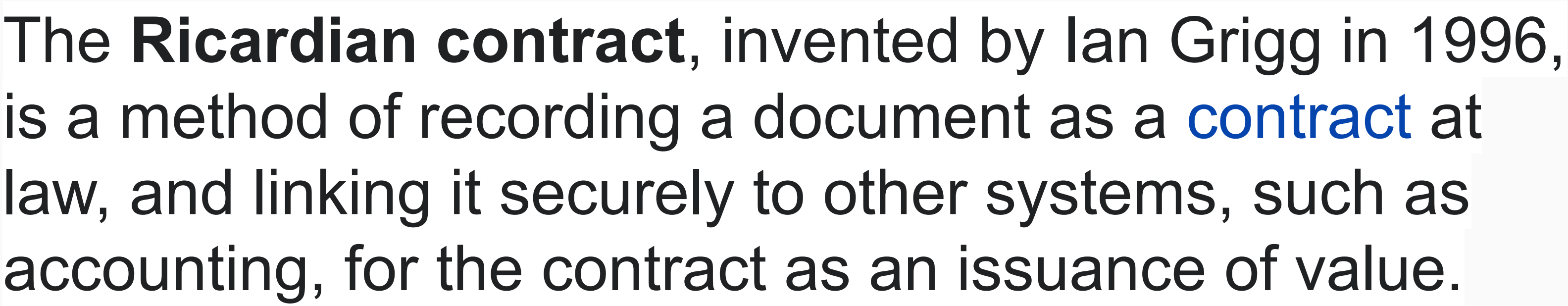
Benefit #4

Graduated disclosure enables credentials to be both more efficient and more privacy-preserving.

#5: Credentials as contracts

The Rules section of an ACDC credential can include a contract that is both human and machine readable and can formally bind the parties to the terms of the data exchange.

In legal circles this is known as a Ricardian Contract. From the Wikipedia page:



The **Ricardian contract**, invented by Ian Grigg in 1996, is a method of recording a document as a contract at law, and linking it securely to other systems, such as accounting, for the contract as an issuance of value.

```
{
  "r":
  {
    "d": "EwY1lkFrn9y2PgveY4-9XgOcLxUdYerzwLIr9Bf7V_NA",
    "warrantyDisclaimer":
    {
      "d": "EXgOcLxUdYerzwLIr9Bf7V_NAwY1lkFrn9y2PgveY4-9",
      "u": "0AG7OY1wjaDAE0qHcgNghkDa",
      "l": "Issuer provides this credential on an \"AS IS\" BASIS, WITHOUT WARRANTIES OR
CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any
warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
PARTICULAR PURPOSE"
    },
    "liabilityDisclaimer":
    {
      "d": "EY1lkFrn9y2PgveY4-9XgOcLxUdYerzwLIr9Bf7V_NAw",
      "u": "0AHcgNghkDaG7OY1wjaDAE0q",
      "l": "In no event and under no legal theory, whether in tort (including negligence),
contract, or otherwise, unless required by applicable law (such as deliberate and grossly
negligent acts) or agreed to in writing, shall the Issuer be liable for damages, including
any direct, indirect, special, incidental, or consequential damages of any character arising
as a result of this credential. "
    }
  }
}
```

NSFM (Not safe for Muggles!)

Features of Ricardian Contracts

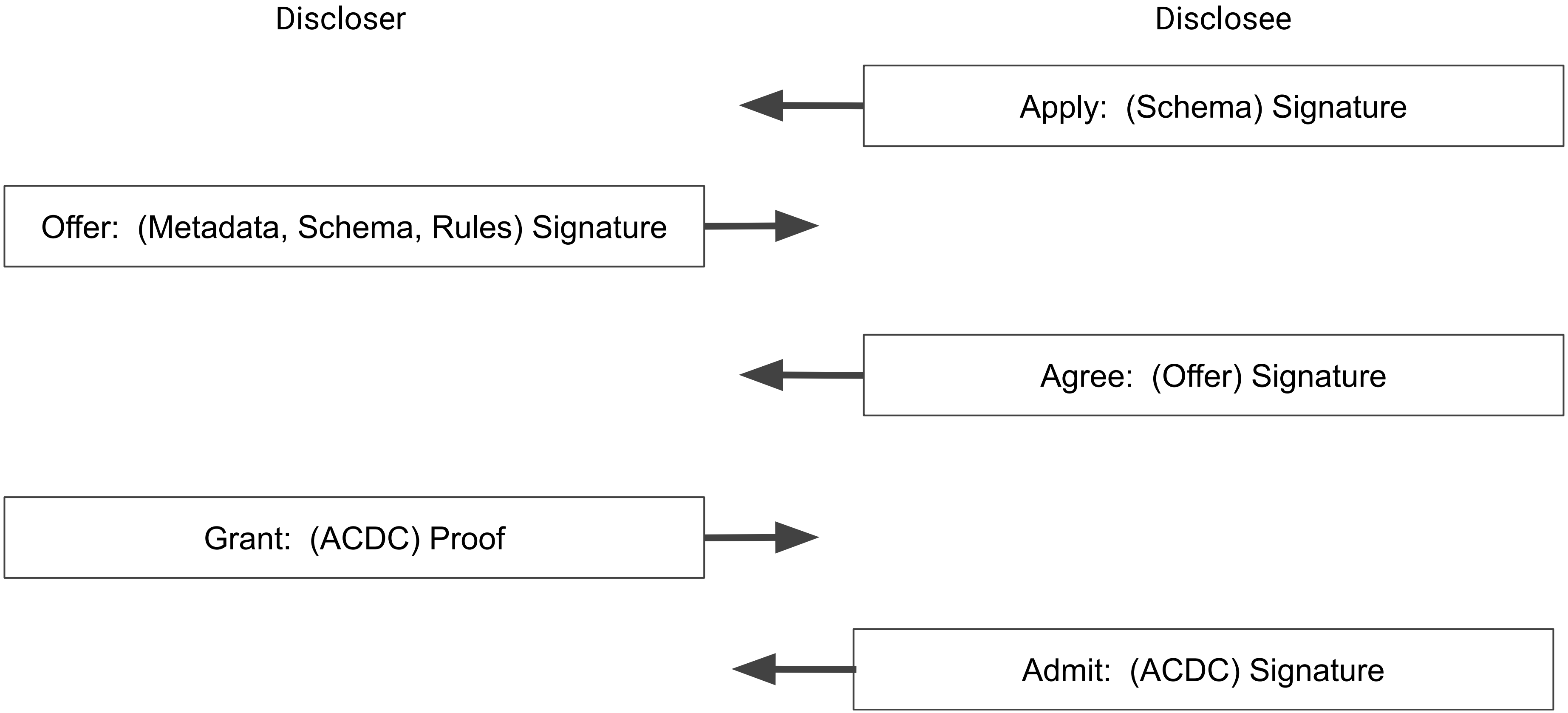
1. Ricardian contracts (not a smart contract!) leverage existing legal language and processes.
2. They can include waivers, terms-of-use, consent, confidentiality, contingencies and so on.
3. With ACDC, every part of the contract can have a SAID.
4. This allows for individualized rules but incentivizes ecosystems to adopt “fair” rules for data exchange.

Benefit #5

ACDC credentials provide a practical way to tie existing legal constructs and processes to the fair exchange of data.

#6: Contractually-protected disclosure

The ACDC exchange protocol enables partial disclosure of information about a credential to enable parties to agree to terms prior to further disclosure.



Discloser

Disclosee

Apply: (Schema) Signature

Offer: (Metadata, Schema, Rules) Signature

Agree: (Offer) Signature

Grant: (ACDC) Proof

Admit: (ACDC) Signature

```
"r":
  {
    "d": "EwY1lkFrn9y2PgveY4-9XgOcLxUdYerzwLIr9Bf7V_NA",
    "Assimilation":
    {
      "d": "EXgOcLxUdYerzwLIr9Bf7V_NAwY1lkFrn9y2PgveY4-9",
      "l": "Issuee hereby explicitly and unambiguously agrees to NOT 
assimilate, aggregate, correlate, or otherwise use in combination with other 
information available to the Issuee, the information, in whole or in part, 
referenced by this container or any containers recursively referenced by this 
container’s edge section, for any purpose other than that expressly permitted 
by the Purpose clause."
    },
    "Purpose":
    {
      "d": "EY1lkFrn9y2PgveY4-9XgOcLxUdYerzwLIr9Bf7V_NAw",
      "l": "One-time admittance of Issuer by Issuee to eat at place on date as 
specified in attribute section."
    }
  }
```

NSFM (Not safe for Muggles!)

Features of contractually protected disclosure

1. Applies the Principle of Least Disclosure to transactions.
2. Allows “chain-link confidentiality” to protect against unauthorized disclosure, use, or correlation.
3. Enables contingent disclosure (escrow)—for example the release of KYC data if the holder breaks the law.
4. Enables a fair exchange of both data and risk between Discloser and Disclosee.

Benefit #6

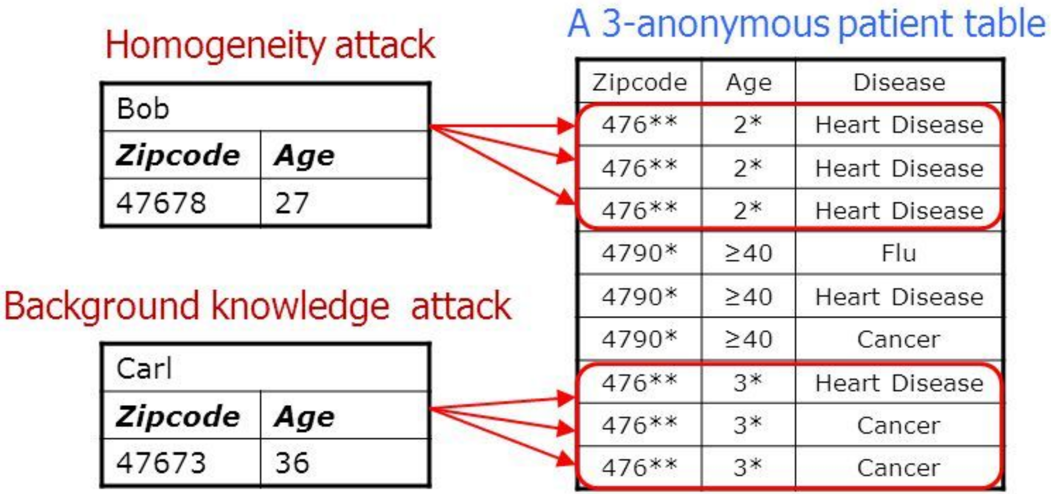
Contractually-protected disclosure is a tool ecosystems can use to enable fair & balanced exchanges of data.

#7: Protection against statistical correlation

ACDC contracts can help protect against a form of personal data exploitation that technology alone cannot protect against: statistical correlation.

Attacks on k-Anonymity

- k-Anonymity does not provide privacy if
  - Sensitive values in an equivalence class lack diversity
  - The attacker has background knowledge



Homogeneity attack

Bob	
Zipcode	***Age***
47678	27

Background knowledge attack

Carl	
Zipcode	***Age***
47673	36

A 3-anonymous patient table

Zipcode	Age	Disease
476**	2*	Heart Disease
476**	2*	Heart Disease
476**	2*	Heart Disease
4790*	≥40	Flu
4790*	≥40	Heart Disease
4790*	≥40	Cancer
476**	3*	Heart Disease
476**	3*	Cancer
476**	3*	Cancer

NSFM (Not safe for Muggles!)

Features of Fair Exchange

1. Most personal data is statistically exploitable. Third parties incentivize second party colluders.
2. ACDC fair exchange contracts can protect against both second party and third party exploitation by placing liability on (de-incentivizing) second party colluders.
3. Enables data exchange to return value to the source.

Benefit #7

ACDC contracts can help restore the balance of power over personal data and return value back to the credential holder and/or issuer.

More questions for Sam?

For more about ACDC and KERI:

https://keri.one

Thank you!

May your keys be with you!