Announcement: Call for Submissions

NSF Convergence Accelerator:

Verified Information Exchange Environments (VIE)

University of Washington Applied Physics Lab
Information Risk and Synthetic Intelligence Research Initiative (IRSIRI)

Contents

I. Overview

We invite you to participate in an experimental, 2-phase crowd-sourced research program being hosted by The University of Washington Applied Physics Lab's Information Risk and Synthetic Intelligence Research Initiative (IRSIRI), in its capacity as a participant in the National Science Foundation's (NSF) "Convergence Accelerator". The 2 phases of the program are described further in the graphic and text below.

The program frames the global information environment as a form of "market" for information that is in need of exchange protocols and local standards setting in order to de-risk, reduce volatility, and increase trust in digital information interactions and transactions. The program aims to create the conceptual foundation for new forms of information "exchange-houses," or verified information exchange environments (VIEs), which would afford stakeholders with the opportunity to increase trust in digital information exchanges through the use of structured ensembles of community-based information sharing, curation, and research tools and data standards with consideration for business, operating, legal, technical, and social (**BOLTS**) concerns.

By way of existing example, payment card systems (for credit cards and debit cards) are VIEs. They make possible the large-scale provision of verified information about identity and other needed information on which parties can rely based on integrated sets of BOLTS requirements that together render the performance of the entire system, including the people and institutional components of the system, more reliable. Vehicular traffic rules are another common example of VIEs.

The program is intended to make progress toward building tools and standards for VIEs that are usable, useful, trusted, and trustworthy.

As part of the first phase of this crowd-sourced research program, the VIE project is hosting open calls for submission of papers, whitepapers, articles, and briefs intended to influence research agendas and the development of VIE-related technologies and future BOLTS standards for VIEs.

Driving questions behind this research program are:

(i) How do we rapidly develop resilient trust in digital contexts?

(ii) What patterns do we make use of, intentionally or unintentionally?

(iii) How do we make sense of information online?

(iv) How can users create trust signals that can be communicated in data?

(v) How can these trust signals be tied not just to individuals, but to individuals in context with subject matter?

(vi) How do we design social systems that self-govern?

(vii) How do we allow for the emergence of neighborhood-watch like mechanisms in the digital information environment?

(viii) What incentives can help facilitate these structures?

Approaches of interest include, but are not limited to, the following as they relate to VIEs:

(i) genuine presence testing of people and things,

(ii) user-centric cryptography,

(iii) decentralized identifiers (DIDs),

(iv) consent sharing and governance,

(v) cryptographically verifiable semantic claims,

(vi) knowledge graphs,

(vii) knowledge and information management,

(viii) self-regulatory business structures,

(ix) organizational psychology,

(x) emerging market dynamics,

(xi) law and regulation,

(xii) adaptive ontology,

(xiii) crowd-sourcing,

(xiv) complexity science,

(xv) serious games,

(xvi) open-source intelligence, and

(xvii) the use of non-fungible tokens (NFTs) and token economics in content sharing, data veracity, and combatting deep-fakes, piracy, and doctored content.

- Program Announcements
    - NSF
    - University of Washington
- Dates
    - Posting Date: October 22, 2021
    - Amendments
        - Amendment 1: October 27, 2021
        - Amendment 2: October 29, 2021
        - Amendment 3: November 15, 2021
    - Deadlines for Submissions
        - Influence Program in Phase I: December 15th, 2021
        - Influence Program in Phase II: April 15th, 2022
        - Inclusion in 2022 Volume: July 15th, 2022
- Contact Information
    - Scott David, Principal Investigator, sldavid@uw.edu
    - R.J. Cordes, Research Coordinator and POC, rj.cordes@cogsec.org

Verified Information Exchanges

If **we want** to address:

- Civil Unrest and Hostile Public Discourse
- Declining Trust in Institutions and Elections
- Food Security and Supply Chains
- Next-Gen Finance and Banking
- Public Health and Welfare

We need an information environment that is:

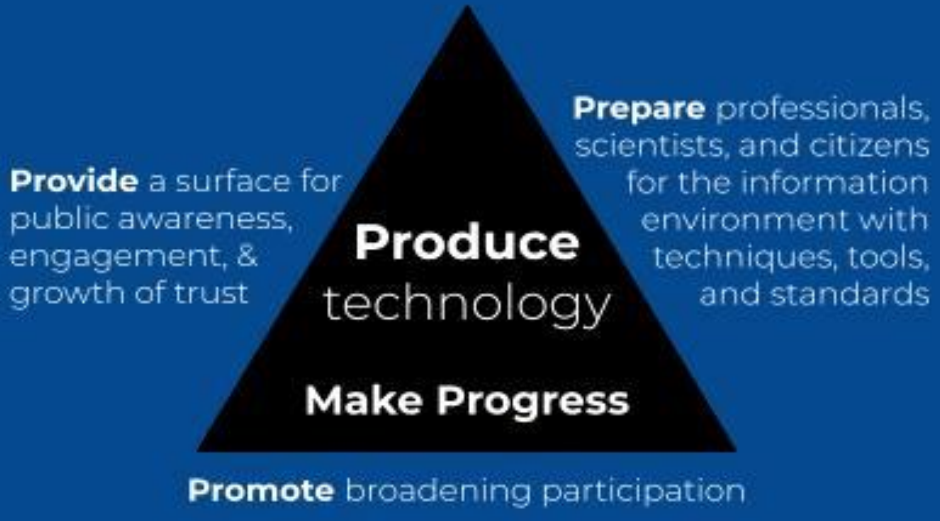
Manageable	Trustworthy	Interoperable
Tools, mentorship, and **skills** to navigate and practice good **stewardship**	**Tools** and **standards** for **governance** and rapid **sourcing** of content and object data	**Comparability** and **standardization** of data, and the methodologies to ensure information quality

Phase I

- **Coordinate** research agendas and technology development
- **Collaborate** between disciplines and backgrounds
- **Communicate** with impacted stakeholders and users

Phase II

- Collect the **Experts** who want to make impact
- **Explore** the problem space
- **Extract** best practices and techniques



Provide a surface for public awareness, engagement, & growth of trust

Produce technology

Make Progress

Prepare professionals, scientists, and citizens for the information environment with techniques, tools, and standards

Promote broadening participation

II. Background

Situation. There is a tragedy of the commons in the global information environment. A well-meaning individual attempting to develop an informed opinion on any topic of the day will encounter a deluge of both possibly relevant and contradicting information from good-faith sources, opportunists, flawed thinkers, and threat actors alike.

This flood of information is generally accessed through tools which were designed for the optimization of dwell-time and emotional engagement creating commercially exploitable network effects that reinforce echo chambers, amplify outrage, and reward discord. The speed and ease with which resharing can occur coupled with the ability and incentives to mask or pervert identity, source, and meaning exacerbates these network effects, contributing to an increasingly hostile and polarized public discourse. This situation has been titled an “Infodemic” by the World Health Organization, “Information Bankruptcy” and “A Failing Trust Ecosystem” by the Edelman Trust Barometer’s 2021 report, and the “Decade of Decreasing Trust” in the Atlantic Council's 2021 GeoTech Commission Report.

Without timely intervention, this situation will only degrade, as deep-fake technology, augmented reality technology, and digital influence operations methodologies are rapidly becoming more sophisticated and accessible. Given the well over 2 million peer-reviewed articles and millions of other reports, datasets, and other media being published and shared yearly, not even experts whose professional responsibilities include managing and evaluating information flows are immune from this Infodemic. New tools are required to help people of all walks of life judge the trustworthiness of the information they receive, separate signal from noise, and be better stewards of the global information environment.

All forms of human exchange, whether it be an exchange of goods or information, are based on trust - trust in process, institutions, or people. Trust is built on actual and perceived notions of reliability, predictability, safety, and security. Historically, where interaction volume and number of participants increases rapidly within a market, the “trust” that was previously engendered by that market starts to break down and is generally followed by the emergence of risk-sharing communities-of-interest in the form of local associations engaging in rule-setting and standardization. A time-tested focus of that emergent, “local” rule-setting and standardization activity has focused on various sorts of “exchange protocols” which provide participants with “signals” of trust and calibrate expectations of risk and benefits more accurately in transactions. For example, trusting that you will be able to find a fair transaction (liquidity), that you will receive what is expected (standards), that you will have recourse in the case you don’t receive what you expect (enforcement), and can feel confident in your choices based on current trends (stability).

While this problem of volatility and declining trust in the global information environment appears to be novel, when examined as a “market” undergoing growing pains from rapidly increasing interaction volumes, decentralization, and competition, the trust challenges can be seen as a new instance of an old problem with novel features.

Goals. Develop tools which assist individuals, communities, and companies in making their shared information environments more manageable, trustworthy, and interoperable.

Approach. The University of Washington Applied Physics Lab’s Information Risk and Synthetic Intelligence Research Initiative (IRSIRI), as a participant in the National Science Foundation’s (NSF) “Convergence Accelerator”, is hosting an experimental, crowd-sourced research program which frames the global information environment as a market for information in need of exchange protocols and local standards setting in order to de-risk, reduce volatility, and increase trust in digital information interactions and transactions. The program aims to create the conceptual foundation for exchange-houses, or verified information exchange environments (VIEs), which would increase trust in digital information exchanges through the use of an integrated ensemble of community-based data standards and information sharing, curation, and research tools with consideration for business, operations, legal, technical, and social (BOLTS) variables reflecting stakeholder concerns. The creation of fully operational VIEs could be a daunting challenge for several reasons:

- A multitude of tools have been recommended to be a part of such an ensemble, such as tools that perform monitoring for influence, measure volatility and trust in digital discourse, manage identity, and facilitate crowdsourcing, among others in myriad use-cases. No single developer could be relied upon to construct or deploy all of them.

- A fundamental aspect of designing adoptable tools is the need to meet the user where they are, this being the case, the ensemble of tools and exchange protocols would need to be developed iteratively with regular feedback from both the research community, potential user-base, and other stakeholders, such as tool developers. Further, it would likely need to "play nice" with the platforms users already choose to use and would likely need to run “behind the scenes” or off these platforms.

- The scientific, engineering, and other professional disciplines that may have valuable input on how a VIE and its tools should operate and may have use for a VIE are diverse and often siloed. Given the potential impacts of a VIE on public discourse and disparate use-cases it is essential that these many disciplines be consulted and considered.

With these challenges in mind, the VIE project is hosting open calls for submission of papers, whitepapers, articles, and briefs intended to influence VIE-related research agendas and the development of VIE-supporting technologies.

Topics of interest include, but are not limited to (i) genuine presence testing of people and things, (ii) user-centric cryptography, (iii) decentralized identifiers (DIDs), (iv) consent sharing and governance, (v) cryptographically verifiable semantic claims, (vi) knowledge graphs, (vii) knowledge and information management, (viii) self-regulatory business structures, (ix) organizational psychology, (x) emerging market dynamics, (xi) law, (xii) adaptive ontology, (xiii) crowd-sourcing, (xiv) complexity science, (xv) serious games, and (xvi) open-source intelligence in order to establish scalable methods for the generation and communication of trust signals. Also of interest is the use of non-fungible tokens (NFTs) and token economics in content sharing, data veracity, and combatting deep-fakes, piracy, and doctored content.

The intent of this open call for submissions is to find both experts and nonexperts who want to make an impact, explore the problem space, and extract insights, best practices, techniques, and frameworks for improving our shared information commons. In addition, this call is intended to help organizations, individuals, teams, and communities interested in making impacts:

1. **Coordinate.** There are too many research areas and solutions for any one team to evaluate alone. For example, law, finance, policy, public health, education, and psychology and many other areas of study all contain insights and requirements relevant to the development of the next generation of information technologies. The submissions process is intended to help professionals, researchers, and developers to coordinate their efforts.

2. **Collaborate.** This is not a traditional call for papers. Any responsible organization, team, or individual is eligible to submit work. Many fields have generalizable concerns and requirements in common; interorganizational and interdisciplinary collaborations which help to generalize patterns of risks, practices, use-cases, and requirements between fields are highly encouraged. Further, rather than simply submitting a paper before the deadline, the submission process for this call allows for (and encourages) your team to collaborate with the VIE team and other teams submitting work.

3. **Communicate.** The technologies and research agendas that this call will help inform and influence are varied and may have wide-reaching impacts. This call is an opportunity to broaden participation and provide an opportunity for those who may be impacted by or use resulting technologies to influence their development and make their voices, perspectives, interests, use-cases, and concerns heard.

For more information on responding to this call for submissions, please see the following sections of this document.

Announcements of the VIE program can be found on the NSF and University of Washington websites.

II. Scope and Type of Submissions Requested

The VIE program has a wide scope both in terms of relevance and format.

A. Scope and Relevance

The VIE program has three current open calls for submissions. Submitted work should be relevant to one or more of these calls. While direct answering of the "driving questions" of each call is encouraged, work which intersects with or informs these questions, answers similar questions, or suggests new, related questions is also welcomed. Please see submission guidelines for more information.

i. Submissions related to (i) signal factors (e.g., roles, titles) involved in digital trust, (ii) communication dynamics of digital communities, (iii) cycles in the capture, qualification, sharing, and synthesis of information in online sensemaking, and (iv) user and content journeys (e.g., content "lifecycles"), in varied domains to consider where tool interventions would be most impactful. The driving questions behind this call for submissions are:

   - *How do we rapidly develop resilient trust in digital contexts?*
   - *What patterns do we make use of, intentionally or unintentionally?*
   - *How do we make sense of information online?*

ii. Submissions related to (i) tagging subject matter, (ii) digital annotations, (iii) curation of information, (iv) creating and sharing "trust signals", indications of veracity or trustworthiness, and (v) the compression and communication of meaning. We are interested to see recommendations of extant or adapted models for labeling and managing relationships and content in digital contexts. The driving questions behind this call for submissions are:

- *How can users create trust signals that can be communicated in data?*
- *How can these trust signals be tied not just to individuals, but to individuals in context with subject matter?*

iii. Submissions related to (i) information-oriented communities of practice (e.g., academic, national security), (ii) private rule-setting, (iii) serious-games frameworks, and (iv) commons stewardship. We are interested in the development of social systems engineering recommendations for encouraging adoption and good-faith use of tools, reducing error propagation, and developing resilience against threat actors within systems that rely on crowdsourcing and stewardship of a commons (e.g., Wikipedia). Token economics, among other topics, may be valuable to explore. The driving questions behind this call for submissions are:

- *How do we design social systems that self-govern?*
- *How do we allow for the emergence of neighborhood-watch like mechanisms in the digital information environment?*
- *What incentives can help facilitate these structures?*

B. Types of Submissions

The goal of submissions is to influence research agendas and technology development. To that end, no particular format, length, or type is requested. Submissions may come in a variety of formats, including, but not limited to, academic articles, literature reviews, white papers, playbooks, field guides, reports, short articles, or briefs. Examples of nontraditional formats might include:

- One-page briefs and “maps of content” which indicate what resources might be relevant from a particular area of research.
- Small briefs by companies addressing the identity and data driven challenges and opportunities in their use-cases and what is needed to address them.
- Cautionary articles which address potential pit-falls and recommendations of what to avoid.
- Articles which offer recommendations related to adding to or adapting the research questions and scope of the program.

If submission process (Section III.A) is followed and requirements (Section III.B) are met, the submission will be considered and processed according to the evaluation criteria (Section III.C).

III. Submission Process and Requirements

The VIE program is making use of a recently formalized methodology known as “catechism-based project management” to inform its submission process. The VIE program is using this methodology so that the submissions it receives can be more usefully integrated and coordinated in this multi-disciplinary and diverse analysis. Complex systems invite complex solutions, and the catechism methodology helps us and relevant stakeholders to tame that complexity and to convert it into new and valuable shared insights about avoidable risks to the benefit of all stakeholders.

A project “catechism” is a simple, version-able document that allows the team and stakeholders to align on expectations without the burden of traditional project documentation. Originally introduced by the Defense Advanced Research Projects Agency (DARPA), catechisms were implemented to improve likelihood of team success, comparability between projects, and optimizing of fit between teams and stakeholders in their work. The VIE program will be using a simplified variant of the “Facilitator’s Catechism”, which was designed for remote teams (see Appendix A for this template).

All submissions related questions and communications should be directed via email to the program’s research coordinator and POC at rj.cordes@cogsec.org.

A. Submission Process

If there is interest in submitting work to the VIE program, please follow the instructions below. If there is interest in submitting already finished work, please see Frequently Asked Questions (Section V).

i. Creation of a Project Catechism

Your team is expected to generate a project catechism (see Appendix A: Project Catechism), which consists of 5 sections, (i) Situation, (ii) Mission, (iii) Approach, (iv) Implications of Outcome, and (v) Administration, Logistics, and Communications. Each contains questions which will help your team clearly communicate the type of submission that will be produced and why. Catechisms can be as long or as short as your team sees as necessary, as long as they answer the questions relevant to the team’s work. See Appendix A for the catechism format and a link to download a template.

ii. Submission of Project Catechism

Once a catechism is created, submit it via email to program’s POC with a link to, or a .docx attachment of, the catechism. Include “Catechism Submission” in the email subject line.

This is done to keep the program aware of what work is being done and what may be submitted. This allows us to inform your team if relevant resources become available or if there are teams working on similar research questions. This also provides an opportunity for your team to receive feedback before substantial work is completed, improving the likelihood of a relevant and impactful submission.

Submission of the catechism does not create an obligation to produce work or to use the approach designated. You, your team, or your organization are free to change a catechism at any time. If substantial changes are made to the team's approach or intended submission, consider contacting the program's POC to improve the likelihood of a relevant and impactful submission.

The team may request an evaluation at any time, of existing work or of the catechism itself by contacting the program's POC. Please include "Evaluation Request" in the subject line of the email.

iii. Final Submission of Written Work

Written work should be submitted via email to the program's POC, in the form of an attached .docx with "Submission" in the subject line. Requirements of submitted work are discussed below.

B. Submission Requirements

All written submissions should be submitted in a .docx, in 12-point font, with limited formatting. The submission should be accompanied by a project catechism and include:

i. One page cover sheet identifying:
    a. Title of the work
    b. Date of submission
    c. Name of the PI, team leader, first author, or sole author
        i. Their affiliation
        ii. Email address
    d. If more than one author, a list of contributing authors and their affiliations, if more than 10 authors, place list on a separate page

ii. An abstract (500-word limit)

iii. At the end of the work, there should be a bulleted list of 3 to 10 recommendations for future research, technology development, or policy decisions

C. Evaluation Criteria

All written submissions will be evaluated by the following criteria:

i. Quality of the writing

ii. The value and potential impact of recommendations for future VIE research, technology development, and policy decisions

iii. The relevance to the research questions posed in the initial call for submissions

D. Eligibility

All responsible organizations, teams, and individuals are eligible to submit work.

IV. Use of Submitted Material

Written work submitted to the program may be formatted and disseminated to partners and collaborators of the program. In addition, the work (or portions thereof) may be selected for:

i. Use, in whole or part, in program-related newsletters and publications,
ii. Dissemination to interested organizations that may or may not be VIE program partners or collaborators,
iii. Inclusion in an end-of-year volume along with other submissions and intended to be presented to the NSF, and
iv. Hosting and/or reference online along with other submissions

To facilitate the use of and reference to submitted work by the program and its many stakeholders, and to assure appropriate attribution to the authors, all submissions to the program should be made pursuant to the Creative Commons license: “Attribution 4.0 International (CC BY 4.0).”

The program recognizes that some limited submissions may not be appropriate for wider publication under the “CC BY 4.0” license; accordingly, authors of such submissions should contact the program’s research coordinator and POC to discuss alternative licensing arrangements PRIOR to making any such submissions.

V. More Information

Questions should be directed via email to the program’s research coordinator and POC at rj.cordes@cogsec.org.

A. Submission Checklist

- Team has read Section II, Scope and Type of Submissions Requested, and Section III, Submission Process and Requirements.

- Team has created a project catechism (see Appendix A).

- Team has submitted the project catechism to the program’s research coordinator and POC with “Catechism Submission” in the subject line.

- Team has a written deliverable which conforms to the Submission Requirements (see Section III.B, Submission Requirements).

- Team has submitted written deliverable to the program’s research coordinator and POC with “Submission” in the subject line.

B. Frequently Asked Questions

- Those interested in submitting already finished work that is either currently unpublished, a preprint, or can be republished, can submit said work without a catechism. See Section III.A for Submission of Written Work, and Section III.B for requirements.

- There is no limit to the number of submissions by an organization, team, or individual.

- There is no mandated style-guide for writing or citations, nor is there a mandate for the inclusion of citations. However, use of references and citations is encouraged.
- Reviews and critiques of other works which are within the scope of the program are allowed and encouraged, so long as the written deliverable fits the submission requirements.
- Each submission will be considered in terms of its own merit, not in comparison with other submissions.
- There is no limit to the number of submissions that will be considered for inclusion in the program.
- Interested individuals, teams, companies, and communities are encouraged to engage with the program and its administrators closely, co-authorship with those involved in the program is allowed.
- Companies which have existing white papers that are within the scope of the program should contact the program's research coordinator and POC to discuss opportunities to adapt these white papers for submission.
- Statements regarding conflict of interest and current funding are encouraged. If an undeclared a conflict of interest or funding source appears to have significantly impacted the work, the program administrators may reject the submission or require resubmission with a declaration.
- Companies which have or are developing technology solutions which may be relevant to the scope of the program are allowed and encouraged to submit work discussing their approaches and available solutions.

Appendix A. Project Catechism

Google Doc Download: Template Link

For more information on catechism writing, please see the Facilitator's Catechism Playbook.

Full Title of Project

Team or Organization Name	xxx
Facilitator/Project Manager	xxx
Contact Information	xxx
Intended Date of Completion	mm-dd-yyyy / Not Yet Known

Situation

What is the nature of the situation or problem the team is addressing?

Mission

Given the situation, what are the team's goals? What needs to be achieved or effectively communicated?

Potential Avenues of Approach

Given the situation, what are the potential or current avenues of approach?
What tools, methodologies, or expertise, alone or in combination, would be of interest to discuss or use? What are the potential risks or limitations?

Implications of Outcome

What would a successful deliverable mean to stakeholders, the situation, and to team members? What else might be affected? What work could or should come next?

Administration, Logistics, and Communications

Who is the person responsible for the project's completion? To whom, if anyone, is the team accountable? What resources and support elements are required or would be impactful? If the team is open to new collaborators, what are the requirements for participation? Under what circumstances will the project close and the team disband? Who are the current collaborators?