Request for Information

Applications and Barriers to Consensus Protocols (ABC)

DARPA-SN-19-10

November 19, 2018

Amendment 1
November 26, 2018

Defense Advanced Research Projects Agency
Information Innovation Office
675 North Randolph Street
Arlington, VA 22203-2114

Request for Information (RFI)

DARPA-SN-19-10

Applications and Barriers to Consensus Protocols (ABC)

I. Introduction

Technologies for distributed consensus protocols have been revolutionized by their prominent role in cryptocurrency and blockchain technologies. These technologies have dramatic implications for the security and resilience of critical data storage and computation tasks, including for the Department of Defense (DoD). At the same time, the concrete applications and security of these technologies for the DoD is unclear. DARPA is interested in better understanding the broader implications that such technologies may play for the DoD. In order to investigate these technologies, DARPA intends to hold a workshop in February based upon responses to this RFI.

Of particular interest to DARPA are so-called "permissionless" distributed consensus protocols, where any individual may join in the computation (in contrast to "permissioned" distributed consensus protocols, which restrict the participants). For the purpose of this RFI, DARPA is solely interested in permissionless distributed consensus protocols. Permissioned distributed consensus protocol topics will be deemed not responsive to this RFI. While there is a substantial amount of publically and privately supported research and development in distributed consensus protocols, DARPA seeks information along several, less-explored avenues of permissionless distributed consensus protocols. Such information could help inform a future DARPA program.

II. Request For Information

The DARPA Information Innovation Office (I2O) requests information on each of the three (3) topics below. Each of these topics will constitute a session at the workshop. Multiple responses are allowed to each topic and/or to different topics; however, each response should address only one (1) topic. Responders with submissions deemed of interest will be invited to a two-day workshop, tentatively scheduled for February 14 and 15 in Arlington, VA. Some responders may be asked to speak at this workshop about the contents of their submission. RFI submitters should have the intent and capability to attend and speak at the DARPA-run workshop if requested based on a review of their RFI submission. DARPA will not provide funding to attend or speak at the workshop.

DARPA does not plan to respond to submissions other than to confirm receipt; if appropriate, submitters may be invited to attend and/or to speak at the workshop. In some cases, DARPA may request additional information and/or facilitate exchanges.

The three ABC topics are: 1) Incentivizing Distributed Consensus Protocols without Money; 2) Economic-Driven Security Models of Distributed Consensus Protocols; and 3) Centralities of Distributed Consensus Protocols. These topics are described in the following paragraphs.

Topic 1: Incentivizing Distributed Consensus Protocols without Money

Permissionless distributed protocols must incentivize various aspects of participation in the protocol. As an example, Bitcoin uses mining (i.e., paying miners) in order to incentivize its own security. This topic focuses on novel means of creating large-scale permissionless distributed consensus protocols without resorting to paying participants in currency (cryptocurrency, fiat currency, etc.). Of note, all means of rewarding participants (e.g., giving them access to computing resources) also constitute a transfer of value; such transfers are within scope of this topic as long as rewards do not consist of money.

Responses in scope for this topic are general methods for the creation of large-scale permissionless distributed protocols without relying on any currency transfers, while also carefully analyzing the value of any service exchanged for incentivizing participation and/or certain behaviors within the cryptocurrency. Of particular interest are methods to build distributed protocols that have general functionality (e.g., beyond the maintenance of a distributed database/ledger).

Topic 2: Economic-Driven Security Models for Distributed Computation Protocols

Notions of economic utility underpin the security of most permissionless distributed consensus protocols, yet such economic notions have traditionally been at odds with the computer science distributed protocols literature. Historically, the computer science literature views distributed computation protocol participants as either "honest" or "malicious." By contrast, economic notions of security recognize that participants act with respect to notions of utility, and users who might otherwise act "maliciously" nevertheless act within certain limited bounds intended to maximize their own utility (e.g., to derive the most currency through specific mining behaviors). At the same time, the computer science community has investigated such notions in a limited manner, particularly with the covert security model and of the concept of "fair" computation in the secure multiparty computation literature.

Responses in scope for this topic are methods that leverage rigorous economic notions to advance theories of security for distributed, permissionless computation protocols. Responses that constitute minor advances to the current state-of-the-art (e.g., the covert security model or current understanding of fair multiparty computation) are not in scope. Of particular interest are approaches that would realistically yield concretely practical implementations.

Topic 3: Centralities of Distributed Consensus Protocols

Permissionless distributed protocols exist as large-scale distributed systems, but may nonetheless have centralized aspects at multiple levels of abstraction, from code homogeneity (e.g., code for wallets, miners, or other services) to network-level topologies (e.g., at the Autonomous System level) to organizational (e.g., there may be only a very small number of sufficiently expert-level or accepted developers for some consensus protocols). Such centralities may greatly impact the cybersecurity of a permissionless distributed consensus protocol regardless of theoretical guarantees.

Responses in scope for this topic are novel analyses, methods to analyze and/or address the centralization of a distributed consensus protocol. Unintended centralities and/or associated mitigations are in scope for this topic. While responses that address specific (high-interest) distributed consensus protocols are in scope, responses with generalizable applications are of particular interest.

III. Submission Format

Submissions shall be limited to **5 pages** (including cover page). All pages shall be formatted for printing on 8-1/2 by 11-inch paper with 1-inch margins, single-line spacing, utilizing Times New Roman font and a font size not smaller than 12 point. Font sizes of 8 or 10 point may be used for figures, tables, and charts. Document files must be Microsoft Word or Adobe PDF format. Submissions must be written in English. All pages should be numbered.

While proprietary and/or limited distribution submissions are allowed, the workshop will be UNCLASSIFIED. Accordingly, any talks or materials for the purpose of discussion will be made available to the general public. Submissions containing proprietary data should have the cover page and each page containing proprietary data marked appropriately. All responses to this RFI must be UNCLASSIFIED.

Each white paper shall consist of the following sections:

a. Cover Page (1 page)

- Organization
- RFI Topic Addressed
- Technical point of contact (name, address, phone and fax number, and email address)
- Administrative point of contact (name, address, phone and fax number, and email address)
- If applicable, security point of contact (name, address, phone and fax number, and email address)
- If applicable, Commercial and Government Entity (CAGE) code[1]

b. Presentation of Capability (limited to 4 pages)

- Goals and Impact: Describe what is being proposed and what difference it will make (qualitatively and quantitatively) if successful. Describe the innovative aspects of the project in the context of existing capabilities and approaches, clearly delineating the relationship of this work to any other projects from the past and present.
- Technical Plan: Outline and address all technical challenges inherent in the approach and possible solutions for overcoming potential problems. Provide appropriate specific milestones (quantitative, if possible) at intermediate stages of the project to demonstrate progress.

[1] A CAGE Code identifies companies doing or wishing to do business with the Federal Government. See http://www.dlis.dla.mil/cage_welcome.asp.

- Capabilities: Provide a brief summary of expertise of the respondant and their associated organization(s). Describe the organizational experience in this area, existing related intellectual property, and any related specialized facilities. List Government-furnished property, facilities, or data assumed to be available. If desired, include a brief bibliography with links to relevant papers, reports, or resumes of key performers. Do not include more than two resumes as part of the white paper. Resumes count against the white paper page limit.

IV. Submission Instructions

Responses may be submitted at any time until December 20, 2018, at 12:00 noon (ET).
Each white paper may address only one topic. UNCLASSIFIED responses should be emailed to ABC@darpa.mil.

V. Eligibility

DARPA welcomes engagement from all responsible sources capable of satisfying the Government's needs, including academia (colleges and universities); businesses (large, small, small disadvantaged, etc.); other organizations (including non-profit); other entities (foreign, domestic, and government); Federally Funded R&D Centers (FFRDCs); minority institutions; and others.

VI. Disclaimer

This RFI is issued solely for information gathering purposes. This RFI does not constitute a formal solicitation for proposals. In accordance with FAR 15.201(e), responses to this RFI are not offers and cannot be accepted by the Government to form a binding contract. DARPA will not provide reimbursement for costs incurred in responding to this RFI, to include attendance at any follow-on workshop or related event. Respondents are advised that DARPA is under no obligation to provide feedback to respondents with respect to any information submitted under this RFI. Response to this RFI is strictly voluntary and is not required to propose to any subsequent solicitations on this topic, if any.

Submissions may be reviewed by the Government (DARPA and partners) and Scientific Engineering and Technical Assistance (SETA) contractors. All personnel with access to the submissions will be covered by a legally-binding, non-disclosure agreement.

VII. Point of Contact

Inquiries should be submitted via email to ABC@darpa.mil.