Opportunity Title: Digital currencies and distributed ledgers
Opportunity Reference Code: IC-16-46

Organization	Office of the Director of National Intelligence (ODNI)
Reference Code	IC-16-46
How to Apply	**Create and release your Profile on Zintellect** – Postdoctoral applicants must create an account and complete a profile in the on-line application system. **Please note: your resume/CV may not exceed 2 pages.** **Complete your application** – Enter the rest of the information required for the IC Postdoc Program Research Opportunity. The application itself contains detailed instructions for each one of these components: availability, citizenship, transcripts, dissertation abstract, publication and presentation plan, and information about your Research Advisor co-applicant.
Application Deadline	4/15/2016 6:00:00 PM Eastern Time Zone
Description	Digital currencies are an emergent technology, typically based on proof-of-work rather than proof-of-value, with a public distributed record of transactions typically maintained in distributed form across a peer-to-peer network rather than centrally. The underlying concept of a “distributed ledger” to maintain a public verifiable authentic record of all transactions has also gained interest as a vehicle for smart contracts, machine-to-machine transactions and as potential support for Open Government initiatives. There are numerous proposals for digital currencies (“Bitcoin” is currently a popular vehicle) and for distributed ledger (“blockchain”). There is active research in the social and economic factors underlying public and political acceptance of such currencies, the social and political impact of their widespread use, and the legal framework that might or should support them. Not so much attention has been paid to security aspects such as the potential threats and risks and the design and assessment criteria appropriate for the security mechanisms (including cryptology). The proposed research lies in two main area. Firstly, what are the criteria by which the security of digital currency and distributed ledger should be assessed, and how should these be expressed in design criteria? Secondly, what are the privacy implications of a public verifiable ledger? Can privacy and anonymity be assured, and if so, how; conversely, what techniques are available now or in the future for the large-scale or well-targeted analysis of transactions and how do they support or inhibit legitimate investigation? **Example Approaches:**

Opportunity Title: Digital currencies and distributed ledgers
Opportunity Reference Code: IC-16-46

Research proposals could consider one or more of the following examples, or identify one not listed below:

Analysis of the risks from a social, economic and political perspective. Scalability and verifiability – possibilities for denial or degradation of service, or compromise of the system as a whole. Whole-system methodologies for assessing the interaction between social and technical components.

Data analysis of a distributed ledger. Mathematical modelling and inference of transactions in general, potential for deanonymization or attribution of transactions, penetration of pseudonymous or partial identities, by legitimate or illegitimate actors.

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Academic Level(s):** Postdoctoral.
- **Discipline(s):**
  - **Business** (11 👁)
  - **Chemistry and Materials Sciences** (12 👁)
  - **Communications and Graphics Design** (6 👁)
  - **Computer, Information, and Data Sciences** (16 👁)
  - **Earth and Geosciences** (21 👁)
  - **Engineering** (27 👁)
  - **Environmental and Marine Sciences** (14 👁)
  - **Life Health and Medical Sciences** (45 👁)
  - **Mathematics and Statistics** (10 👁)
  - **Other Non-Science & Engineering** (13 👁)
  - **Physics** (16 👁)
  - **Science & Engineering-related** (1 👁)
  - **Social and Behavioral Sciences** (28 👁)