Offre n°2024-07575

Consensus-less receiver-anonymous money transfer solution.

Type de contrat : Fixed-term contract

Contrat renouvelable : Oui

Niveau de diplôme exigé : Graduate degree or equivalent

Autre diplôme apprécié : PhD

Fonction : Temporary scientific engineer

A propos du centre ou de la direction fonctionnelle

The Inria Rennes - Bretagne Atlantique Centre is one of Inria's eight centres and has more than thirty research teams. The Inria Center is a major and recognized player in the field of digital sciences. It is at the heart of a rich R&D and innovation ecosystem: highly innovative PMEs, large industrial groups, competitiveness clusters, research and higher education players, laboratories of excellence, technological research institute, etc.

Contexte et atouts du poste

This development project lies partly in the context of the PriCLeSS Proof-of-Concept action (https://project.inria.fr/pricless) led by Davide Frey (WIDE team) and funded by the Cominlabs LabEX (https://cominlabs.inria.fr/) and partly in the context of the SOTERIA H2020 project. The PriCLeSS project establishes a cross-disciplinary partnership to understand the legal challenges and address the technical obstacles associated with data storage in a blockchain context. SOTERIA focuses on the secure management of personal data and on decentralized identity management without relying on classical blockchain technology.

In this context, we are proposing a novel algorithm for asset transfer (cryptocurrency) that has three noteworthy properties, namely consensus-freedom, cost-effectiveness, and quasi-anonymity. Consensus-freedom means the system does not rely on a total order on asset transfers. Cost-effectiveness means that processes only need to store their own asset transfers and some short, constant-size control data. Quasi-anonymity means that no information is leaked on the asset transfers' receivers and amounts, and that the asset transfers' senders can be obfuscated with high probability. As far as we know, it is the first asset transfer system that satisfies all these properties at once. To obtain them the article considers new distributed objects such as agreement proofs as well as well-known techniques such as commitment objects, zero-knowledge proofs, and cryptographic accumulators.

Mission confiée

This engineering position involves implementing the aforementioned asset transfer solutoin. In this task the engineer will be guided by the team who have been working on the algorithm design. The engineer will also have the opportunity to collaborate with other partners from the PriCLeSS and SOTERIA projects.

Principales activités

The engineer will follow the following approximate timeline.

- M1: Analysis of the state of the art:
  - Analysis of existing Money Transfer implementations.
  - Research papers on Money Transfer including the one on the proposed algorithm
- M2: High-level design of the implementation.
- M4: Zero Knowledge-Proof Implementation
- M6: Complete algorithm implementation
- M8: First version of the interface around the algorithm
- M12: Final release of the Money Transfer system.

Compétences

Technical:

- Proficiency in Rust or willingness to learn the language and use it.
- At least basic terminal usage: bash or other environments
- Familiarity with git

Non technical:

- Fluent written and spoken English
- French can be a plus
- Ability to work in a team
- Flexibility
- Planning and ability to meet deadlines

Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Possibility of teleworking (90 days per year) and flexible organization of working hours
- Partial payment of insurance costs

Informations générales

- **Thème/Domaine :** Distributed Systems and middleware
  Software engineering (BAP E)
- **Ville :** Rennes
- **Centre Inria :** Centre Inria de l'Université de Rennes
- **Date de prise de fonction souhaitée :** 2024-07-01
- **Durée de contrat :** 12 months
- **Date limite pour postuler :** 2024-05-14

Contacts

- **Équipe Inria :** WIDE
- **Recruteur :**
  Frey Davide / davide.frey@inria.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

L'essentiel pour réussir

You are interested in systems programming, blockchain, and distributed systems. You are not afraid to design and implement large pieces of software. You can clearly write documentation in English.

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

Please submit online : your resume, cover letter and letters of recommendation eventually

For more information, please contactdavide.frey@inria.fr

Sécurité défense :
Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :
Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation

de handicap.