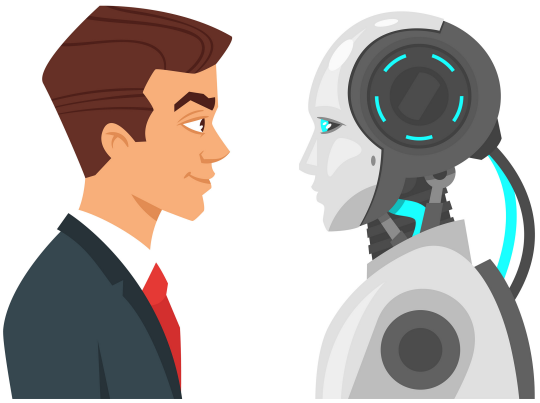
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

Scalable Proof-of-Personhood

Proof-of-Personhood [Bor+17] has the potential to enable a wide variety of novel applications, such as new forms of governance, better resource allocation, and improved online deliberation. Such applications could become especially impactful in an era with AI agents expected to become more prominent.



Encointer [The24] has developed and implemented a highly decentralized proof of personhood (PoP) system relying on key signing parties to provide a secure mechanism for proving the participants' unique personhood and preventing Sybil attacks on autonomous local currencies.

In this thesis, the goal is to explore other, more scalable alternatives to PoP, with the goal to accomodate many more users. We want to investigate eIDs, ePassports, and privacy-enhancing technology (trusted execution environments and/or zero-knowledge proofs) and how they might enable scalable PoP.

Requirements: An interest and experience in cryptography or distributed systems is a plus. We will have weekly meetings to discuss open questions and determine the next steps.

Interested? Please contact us for more details!

Contact

- Malik El Bay: malik.elbay@dezentrum.ch, Dezentrum
- Alain Benzikofer: alain@encointer.org, Encointer
- Yann Vonlanthen: yvonlanthen@ethz.ch, ETZ G97

References

[Bor+17] Maria Borge et al. "Proof-of-personhood: Redemocratizing permissionless cryptocurrencies". In: *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE. 2017, pp. 23–26.

[The24] The Encointer Team. *Encointer: A Proof-of-Personhood Protocol for Local Community Currencies and Universal Basic Income*. https://encointer.org/. 2024.