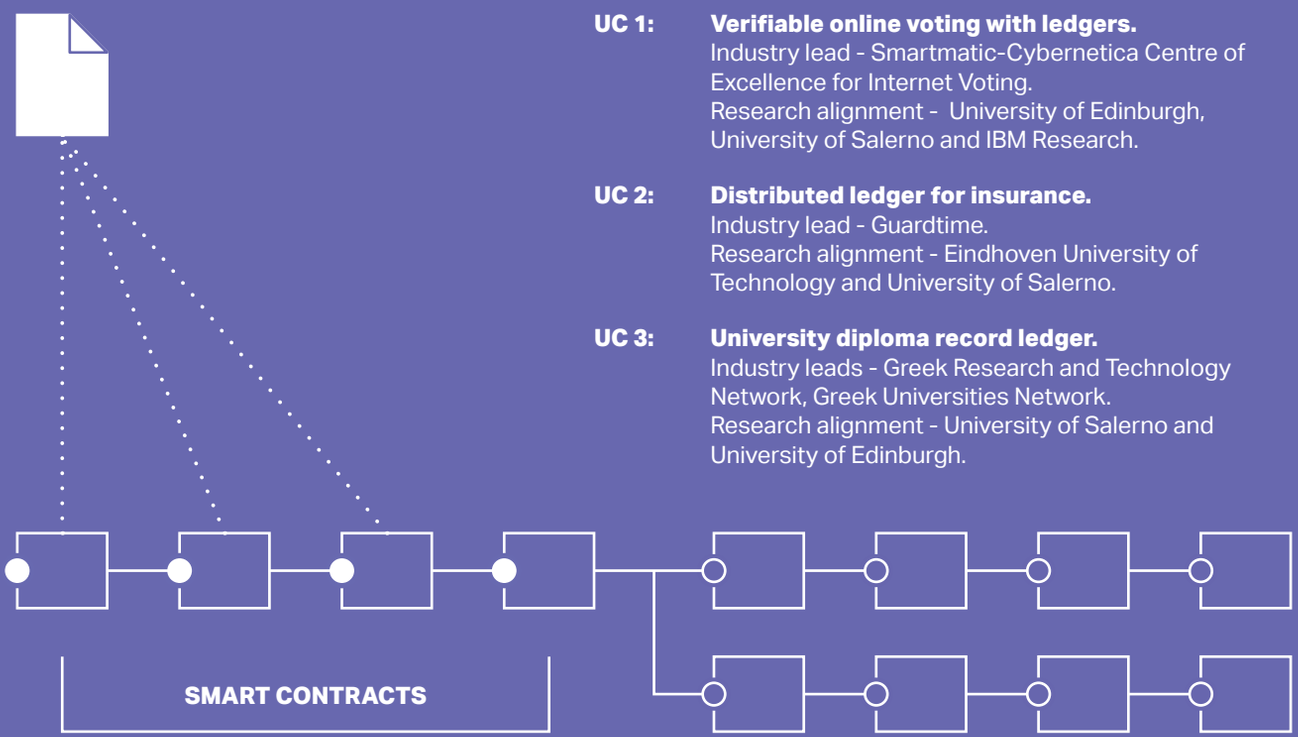
PRIVILEDGE

USE CASE 1:

"E-VOTING" VERIFIABLE ONLINE VOTING WITH LEDGERS

PRIVACY ENHANCING CRYPTOGRAPHY IN DISTRIBUTED LEDGERS

PRIViLEDGE has the ambitious goal to increase the trustworthiness of European ICT services and products and the competitiveness of the European cryptography industry. PRIViLEDGE focuses on enhancing strong cryptographic solutions for privacy in distributed ledgers. To demonstrate its wide scope of applications, PRIViLEDGE works with four different use cases to develop and showcase cryptographic schemes and protocols for privacy and security.



UC 1: **Verifiable online voting with ledgers.**
Industry lead - Smartmatic-Cybernetica Centre of Excellence for Internet Voting.
Research alignment - University of Edinburgh, University of Salerno and IBM Research.

UC 2: **Distributed ledger for insurance.**
Industry lead - Guardtime.
Research alignment - Eindhoven University of Technology and University of Salerno.

UC 3: **University diploma record ledger.**
Industry leads - Greek Research and Technology Network, Greek Universities Network.
Research alignment - University of Salerno and University of Edinburgh.

UC 4: **Update mechanism for Cardano stake-based ledgers.**
Industry lead - Input Output Research.
Research alignment - University of Edinburgh and IBM Research.

* Use cases 1–3 use the immutability of DLT for storing data. Use case 4 enhances DLT with mechanisms for consistent updates.

THE STORY

Fair voting is one of the building blocks of modern democratic societies, and hence trustworthiness of a voting method is of crucial importance. Unfortunately, the requirements put to elections are partly contradictory. From the transparency point of view, we need universal verifiability, meaning that everyone should be able to check that all votes cast by eligible voters have been counted correctly. From the privacy point of view we must not disclose individual preferences of voters to anyone. In fact, it has been shown that the property of universal verifiability is not, under standard assumptions, achievable together with unconditional privacy, nor receipt-freeness.

THE DARE

In order to achieve universal verifiability we need to have a way to publish data from the voting system to those who want to carry out the verification, moreover, we need to convince the verifiers on the authenticity and integrity of the data.

A theoretical construct often used in verifiable voting protocols is a distributed bulletin-board that is publicly readable, with authenticated append-only messages. DLT has very similar goals - can we use this to make deployment of bulletin-boards in truly distributed manner accessible to election organizers and potential verifiers?

Second part of the equation is the data - once made available over public channels, it is near impossible to control what happens in the future. How can we be sure that we are not sacrificing voter privacy in the pursuit of transparency?

THE DO

The prototype voting system implemented in PRIVILEDGE shows how DLT can be put to use for enabling verifiable online voting to achieve meaningful level of universal verifiability under the condition of voter privacy. Together with accompanying audit tools and procedural guidelines it shows how instead of trusting single service provider, it is possible to independently verify the correctness of the voting result in privacy preserving manner.

INTERESTED IN LEARNING MORE ABOUT "E-VOTING" USE CASE ?

- Your primary contact is Sven Heiberg from Smartmatic-Cybernetica Centre of Excellence for Internet Voting OÜ, e-mail: **sven@tivi.io**.
  For any questions or proposals you might have, he's happy to listen.

Follow PRIViLEDGE homepage and Twitter for news and updates.

- **priviledge-project.eu**
- **twitter.com/PRIViLEDGE_EU**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477