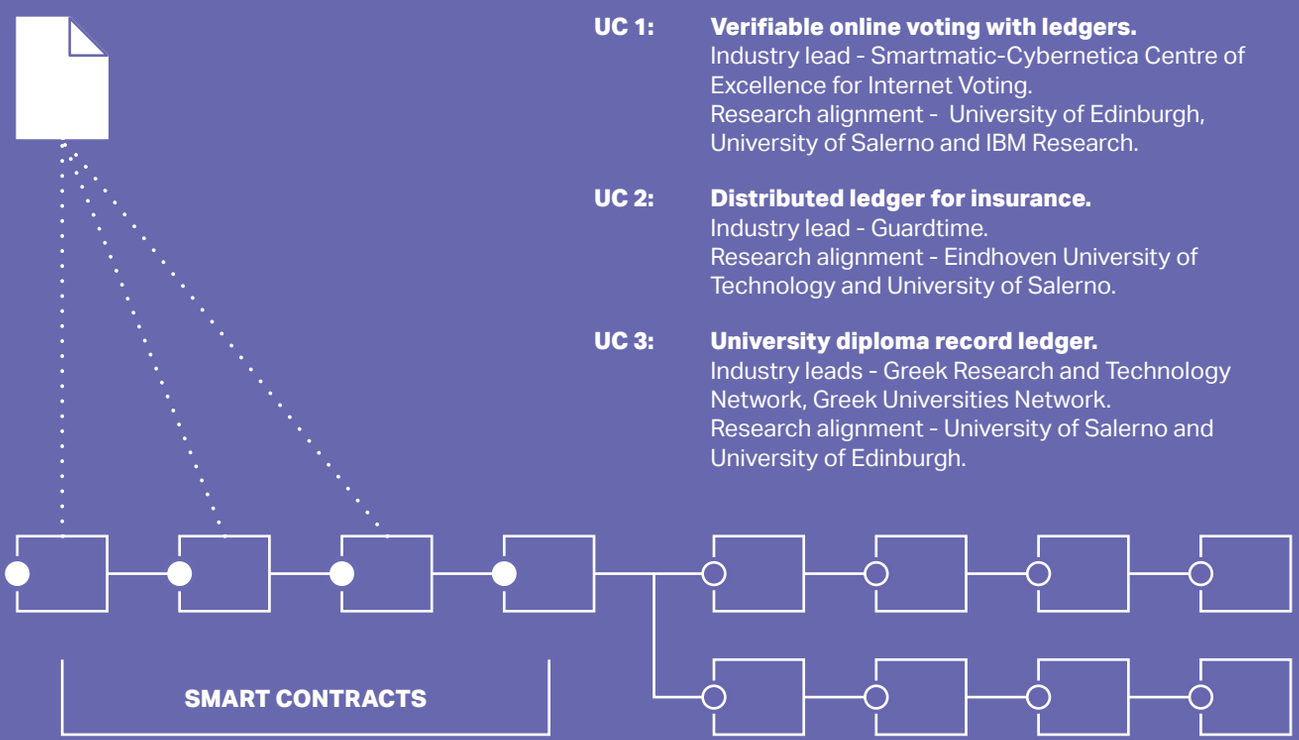
PRIVILEDGE

USE CASE 4:

UPDATE MECHANISM FOR CARDANO STAKE-BASED 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

No matter how carefully any complex software system will be designed and implemented, there will always be a need for future updates and improvements when new requirements arise, bugs are discovered, standards or protocols change, or new technologies become relevant.

Traditionally, such software updates have been handled in an ad-hoc, centralised manner. Meaning that somebody, often a trusted authority, or the original author of the software, provides a new version of the software, and users download and install it from that authority's website (or they don't).

Public ledger systems, although decentralized by nature, very often follow a centralized approach for software updates. So, there is a lot of room for improvement, especially in the decentralization aspect of the update systems used today.

The traditional way of handling software updates is neither decentralised nor secure, nor does it apply the decentralisation and security achieved by modern blockchain technology to the handling of updates for the systems themselves.

THE DARE

At present, there is no standard way to propose software system updates and reach consensus on such proposals. Even when a consensus has been reached, this is usually an informal "social" consensus, and is not the outcome of a secure update protocol, which stores its events in the immutable blockchain history. Moreover, the final decision for the activation of changes is always up to the code maintainer (i.e., a central authority). In addition, the authenticity and safety of the downloaded software is usually verified by the digital signature of a trusted authority, such as the original author of the software.

Also, there is no way to guard against malicious proposals on the one hand, while on the other hand enabling critical security updates or bug-fixes to be distributed in swiftly and do this in a decentralised setting.

Ideally, each participant (with sufficient stake) of the Cardano ledger should be allowed to make update proposals and have a vote on them, then deploy a corresponding update efficiently.

Alas, there are many problems to tackle before this can be achieved, e.g:

- How can we remove decision making on software updates from the central authority and hand it over to the stakeholders community?
- How can we be sure that a malicious proposal will not be approved and at the same time, a beneficial proposal cannot be blocked?
- How can we activate consensus protocol changes on the blockchain without risking a chain split?
- How can we replace the central authority role of the code maintainer by the stakeholder community and still achieve the same guarantees upon the approval of new code?
- How can we leverage the blockchain itself, with its "built-in" consensus mechanism, to handle proposals, voting and deployment of updates?
- How can "concurrent" proposals be handled, preventing contradictory ones from being accepted and deployed at the same time?
- How can we apply a metadata-driven update policy and avoid a one-size-fits-all approach?

THE DO

PRIViLEDGE defines a novel decentralized software updates framework for stake-based ledger systems. This framework follows a holistic approach and examines a software update throughout its whole lifecycle. All the phases in the lifecycle of a software update in the centralized setting have been studied and "decentralized alternatives" for all of them have been proposed by the Priviledge team.

Moreover, the decentralized software updates activation problem has been formally defined and a protocol that offers a solution has been proposed. **By developing the mathematical foundations of decentralised software update systems and implementing a research prototype based on those foundations, managing software updates on public ledger systems will be greatly simplified but even more importantly become essentially decentralized**.

INTERESTED IN LEARNING MORE ABOUT "CARDANO LEDGER" USE CASE ?

Your primary contact is Nikos Karagiannidis, from Input Output Research (IO Research), e-mail: **nikos.Karagiannidis@iohk.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