Privacy-preserving Digital Identity Management

Roman Vitenberg

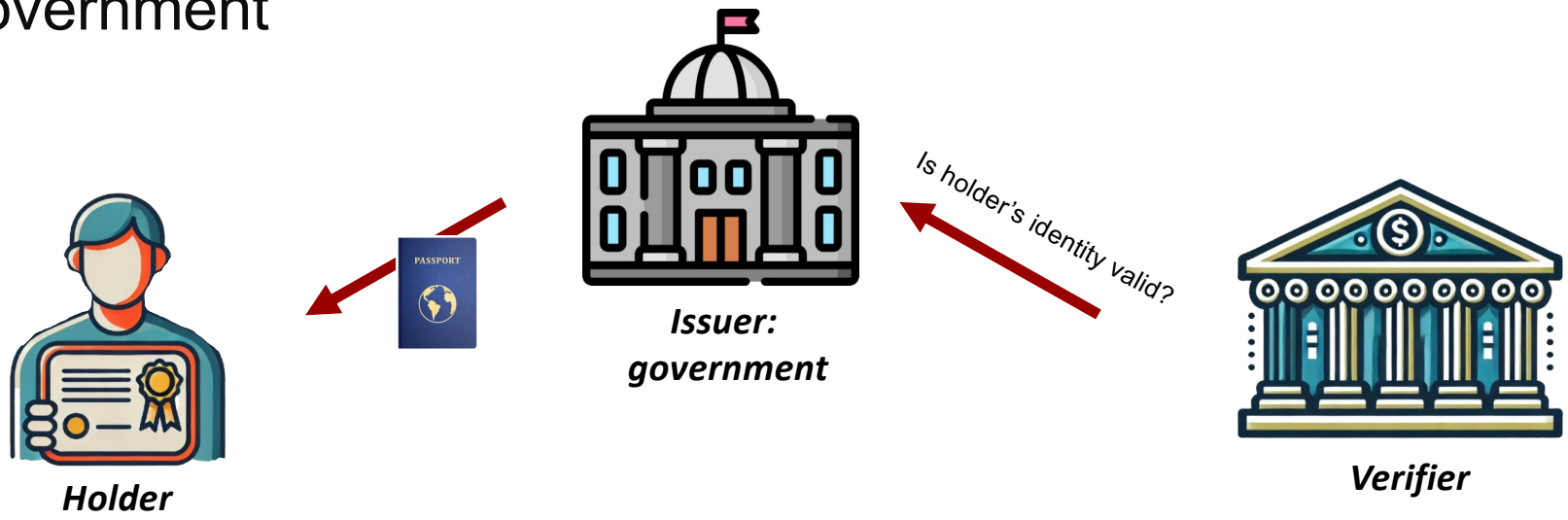
UiO : University of Oslo

A view of someone with one leg in

- Multiple researchers asked me about the scope of DSN and the WG
  - (I am not the right person, but it does not stop people from asking!)
- Keywords used by those researchers
  - Resilient networking
  - Robust systems
  - Decentralized trust
- So, what is the emphasis on?
  - Layers (hardware and software vs networking)?
  - Modelling methodology?
  - Application domains?

Digital identity management: from centralized to federated to self-sovereign

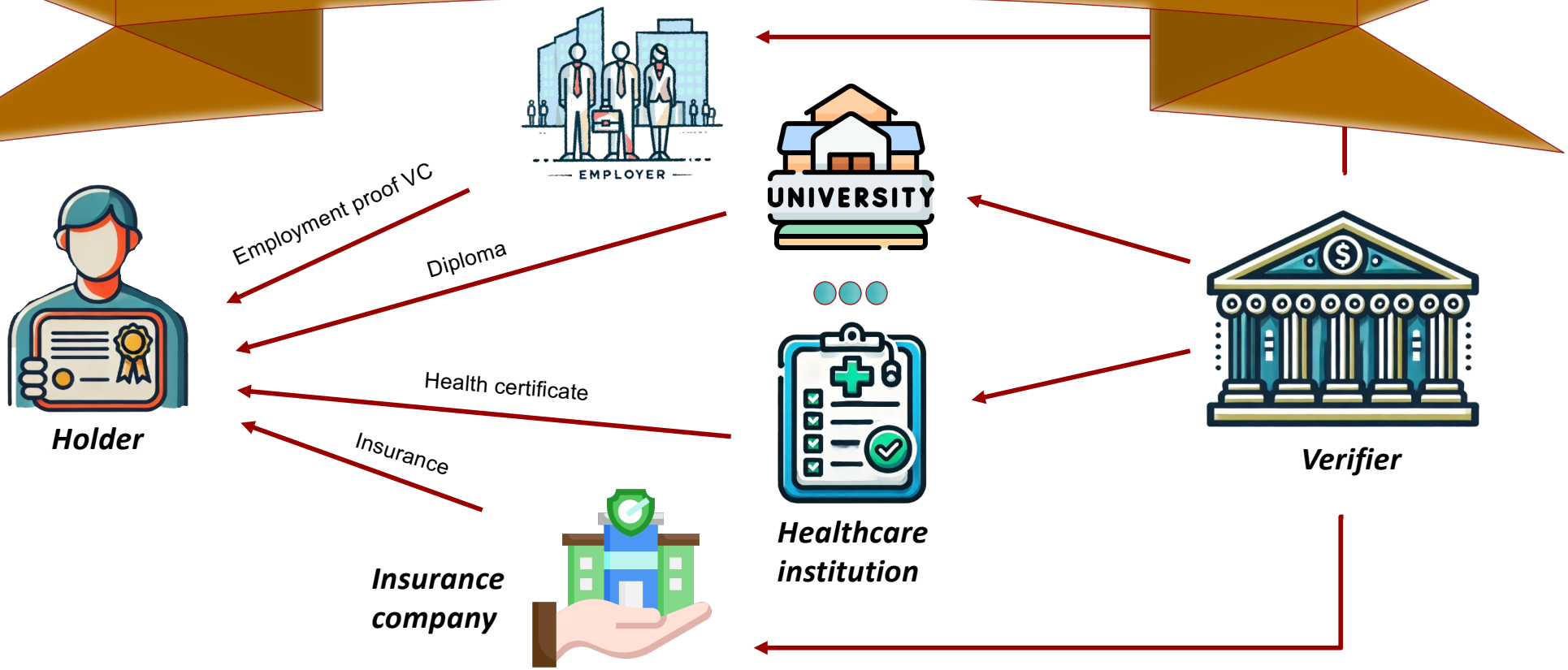
- Classic centralized model: A few verifiable credentials (VCs) issued by the government



Problem: issuers are numerous, inherently decentralized, and multifaceted

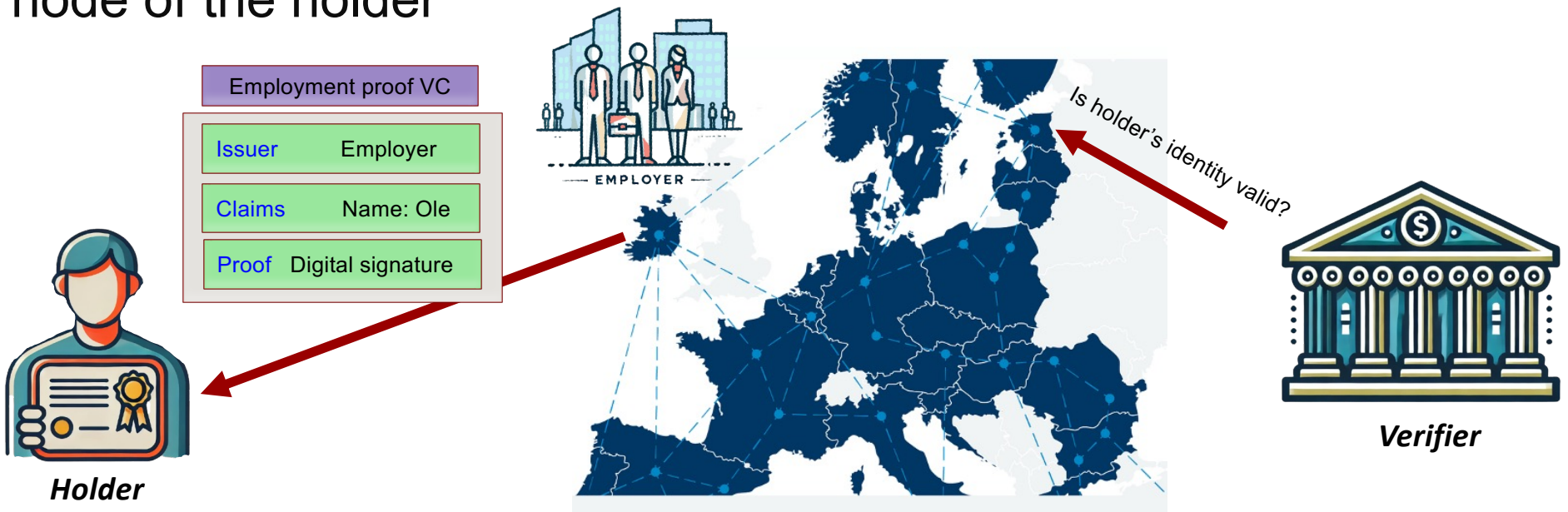
Digital identity management: Multiple silo model

- Each issuer has its own rules, schemas, access control, etc.
- Gives too much control to issuers who can collect information about individual holders



Digital identity management: Federated model

- Each country authorizes issuers in that country
- Each country has a node storing VCs issued in that country
- A verifier contacts the node of the holder



Digital identity management: Analysis of the federated model

Advantages

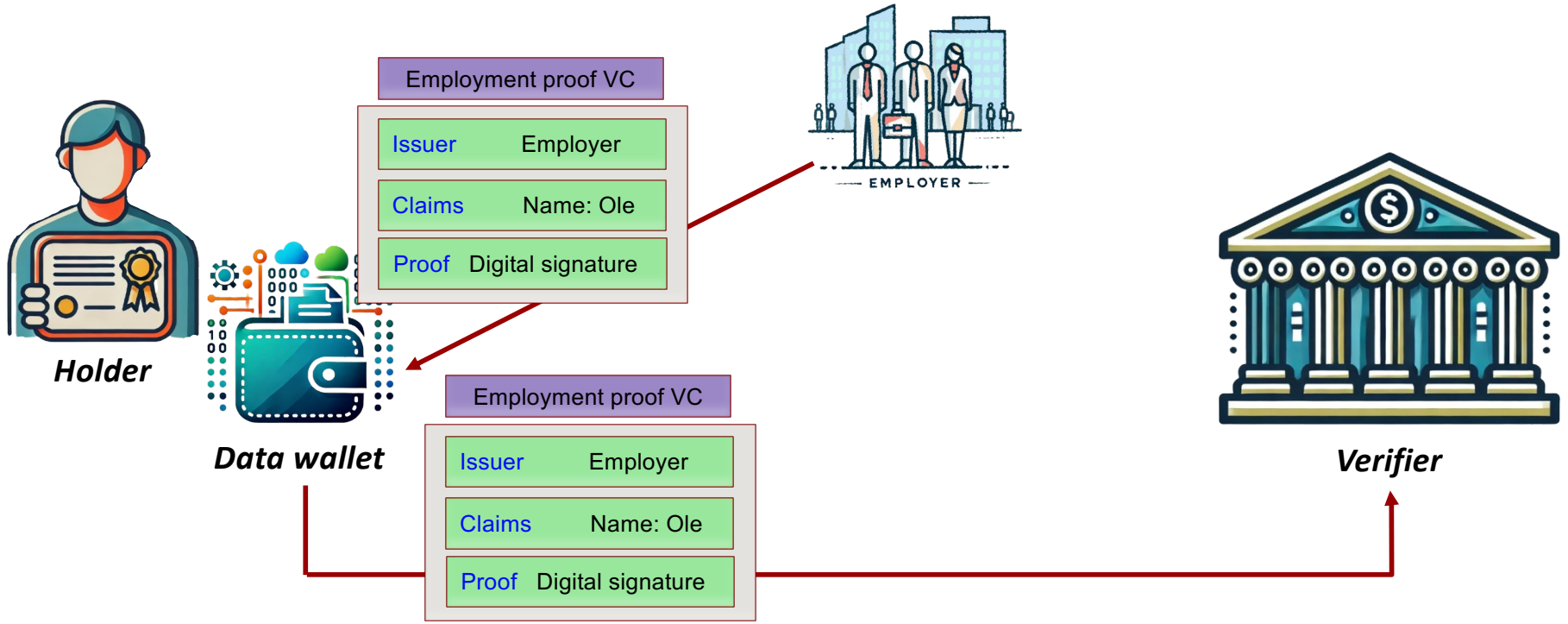
- Enforces homogeneity
- Issuers do not participate in the verification
  - Important for scalability
  - Issuers cannot learn about the verification

Shortcomings

- Government still needs to be in control of issuers
- Holders do not participate in the verification
  - No control about the sharing
  - Not informed about a verification attempt

Digital identity management: SSI model

- Each holder has a data wallet to keep his/her VCs
- A holder may decide to share the VC with individual verifiers
- A verification process involves global public registry accessible to all



Some of the central SSI Principles

- Control: subjects have complete control over the storage and sharing of their identities
- Portability: subjects have the ability to move their identities from one storage platform to another.
- Minimization: when identity data is disclosed, the disclosure should involve the minimum amount of data necessary for verification.

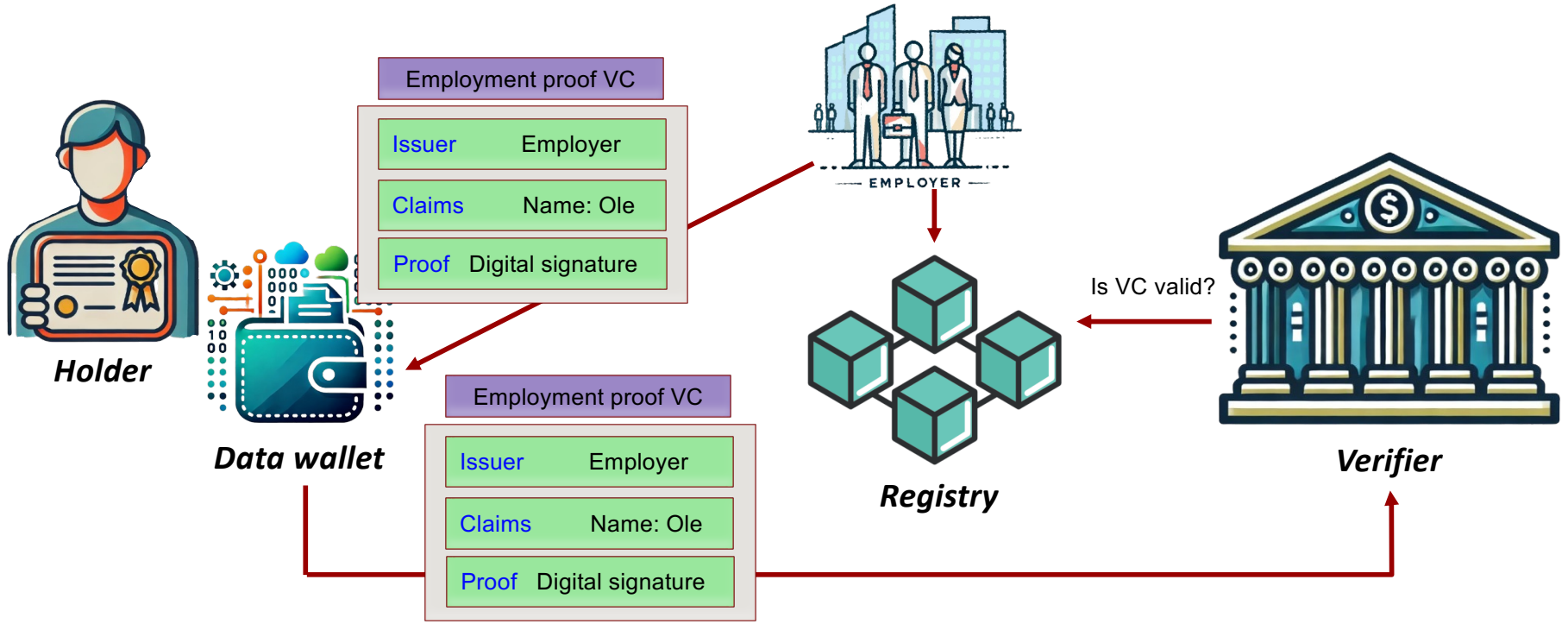
Digital identity management: Advantages of the SSI model

Advantages

- Standardized VC schema and verification procedure
- Enforces homogeneity
- Issuers do not participate in the verification
- Holders decide on sharing information
  - Which verifier?

Introducing validity period and revocation

- Support for validity period determined by the issuer
- Support for revocation (to avoid reissuing short-lived VCs frequently)
- Need for the registry
  - Issuer stores validity tokens, verifier performs verification using those tokens.



A major challenge for the SSI model

Challenge: how to manage the registry?

"Decentralization Trends in Identity Management: From Federated to Self-Sovereign Identity Management Systems", Computer System Review 2025, Praveensankar Manimaran, Thiago Garrett, Leander Jehl, and Roman Vitenberg

A framework for time-limited verification

- For how long can a verifier check the VC validity?
  - The straightforward option of VC validity period is not good for many use cases
  - It would be great to allow it to be configurable by the holder
- How to implement a verification period controlled by the holder
  - A holder shares keys with the verifier that allow interpreting info in the registry
  - An issuer periodically refreshes the info in the registry
  - Bad idea for a holder to send short-lived keys to the verifier
    - Not scalable and requires the holder's device to be always online

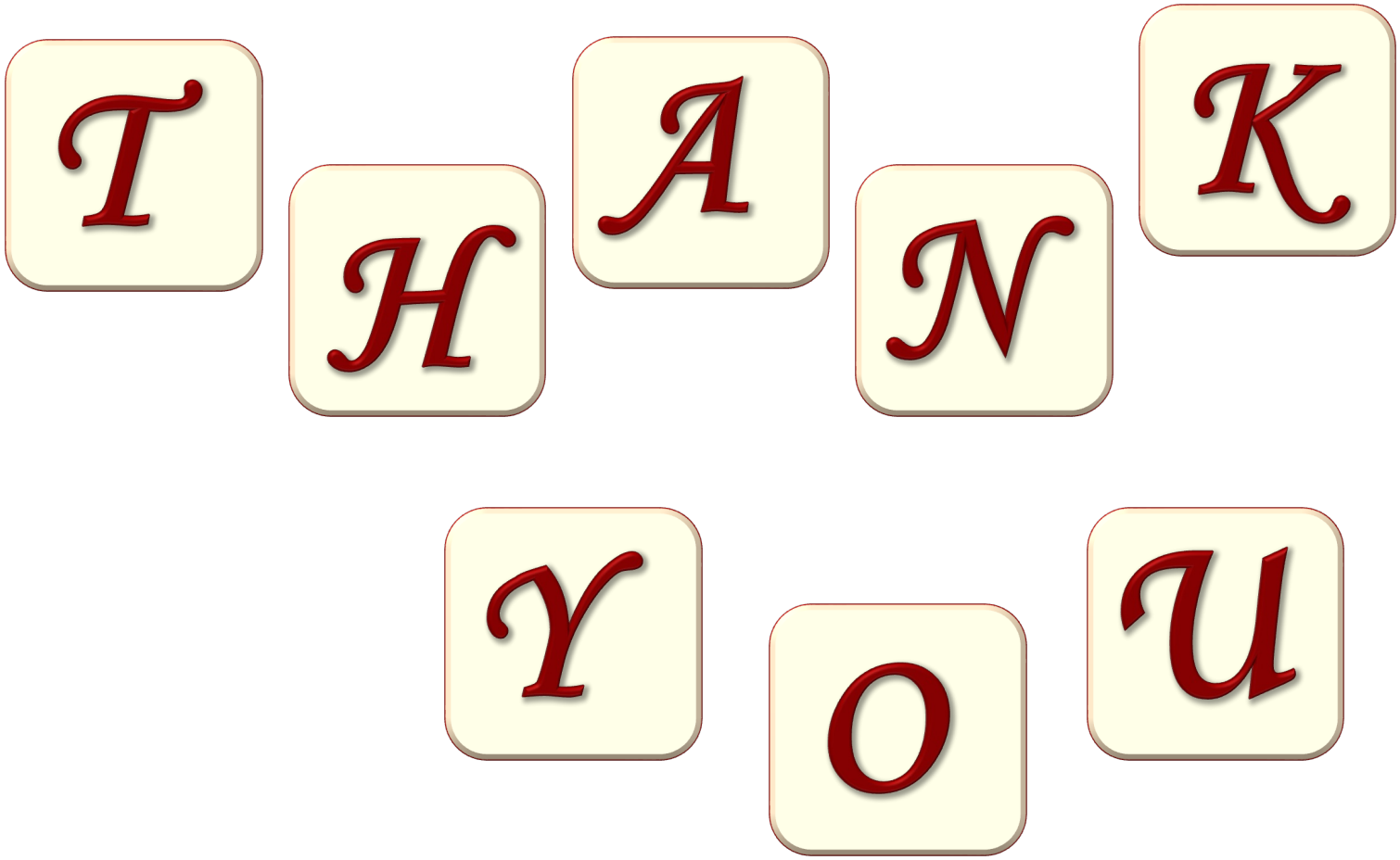
How to design the protocol?

- What tokens to store in the registry and how to use them for verification
  - The standard approach is for each issuer to store in the registry a whitelist of tokens corresponding to the valid VCs produced by this issuer.
  - Since the whitelist is long, it needs to be compacted using, e.g., accumulators.
  - Unfortunately, whitelist compaction does not reduce bandwidth consumption, and it is not clear how to implement configurability of the verification period.
- Additional confidential information
  - Revocation rate by the issuer (”Prevoke: Privacy-Preserving Configurable Method for Revoking Verifiable Credentials”, IEEE Blockchain 2024)
  - Validity/revocation status of individual VCs

The overview of our solution

- Storing a blacklist of revoked tokens in the registry
  - The revocation rate is typically much lower than the issuance rate.
- The registry has access control for writing, but not for reading.
  - If the registry colludes with issuers, issuers will not be able to detect verification.
- The time is divided into epochs.
  - The verification period is measured in epochs.
- An issuer stores the list of tokens in the registry when an epoch starts.
- A holder shares a VC with a verifier once, w/o further communication.
  - Sends multiple tokens, one for each epoch of allowed verification.
  - A token proves non-inclusion in the blacklist using zero-knowledge tech.

"zkRevoke: Configurable Untraceability for Verifiable Credentials using ZKPs", Praveensankar Manimaran, Mayank Raikwar, Thiago Garrett, Arlindo F. da Conceição, Leander Jehl, and Roman Vitenberg, to appear in PETS 26


Т
Н
А
Н
К
У
О
Ц