Security Insights on Retail CBDC e-krona pilot

ITU 2021-11-19

Ian Vitek

CBDC Security

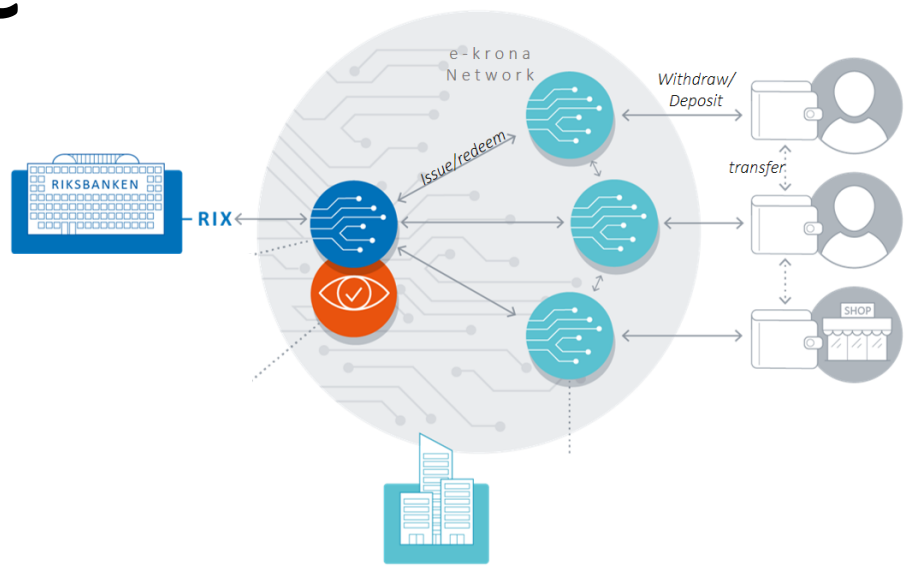
Central bank of Sweden, Sveriges Riksbank

Security Insights on Retail CBDC e-krona pilot

Introduction

Token selection, performance and privacy

Operational security challenges



So where do we start?

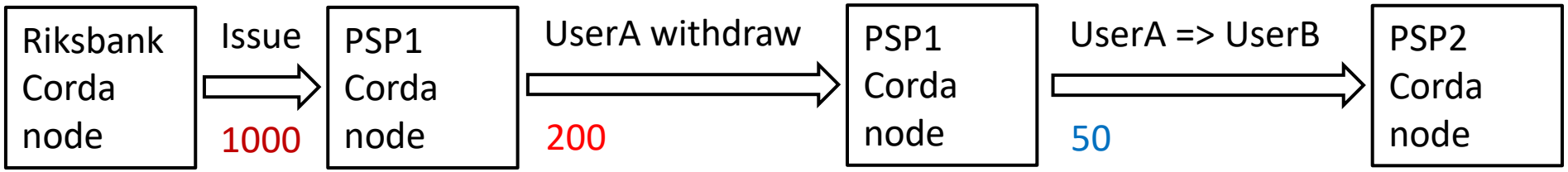
Ian Vitek

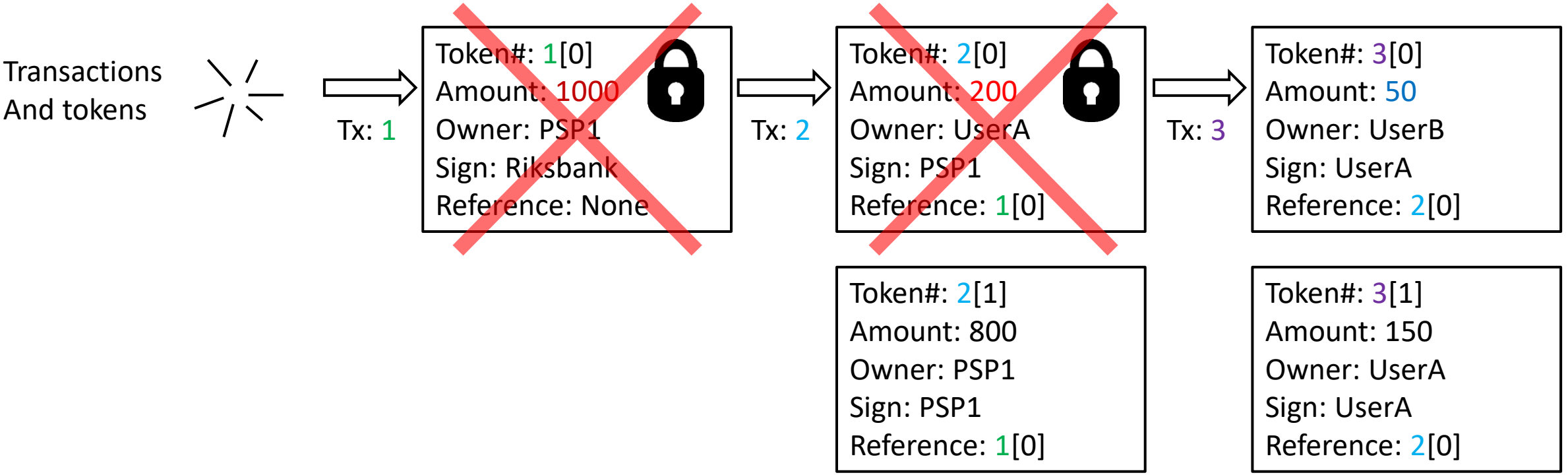
- Started with pentests 1996.
- Interested in web application security, network layer 2 (the writer of macof), DMA attacks and local pin bypass attacks (found some on iPhone).

Employed at Sveriges Riksbank (Central bank of Sweden).

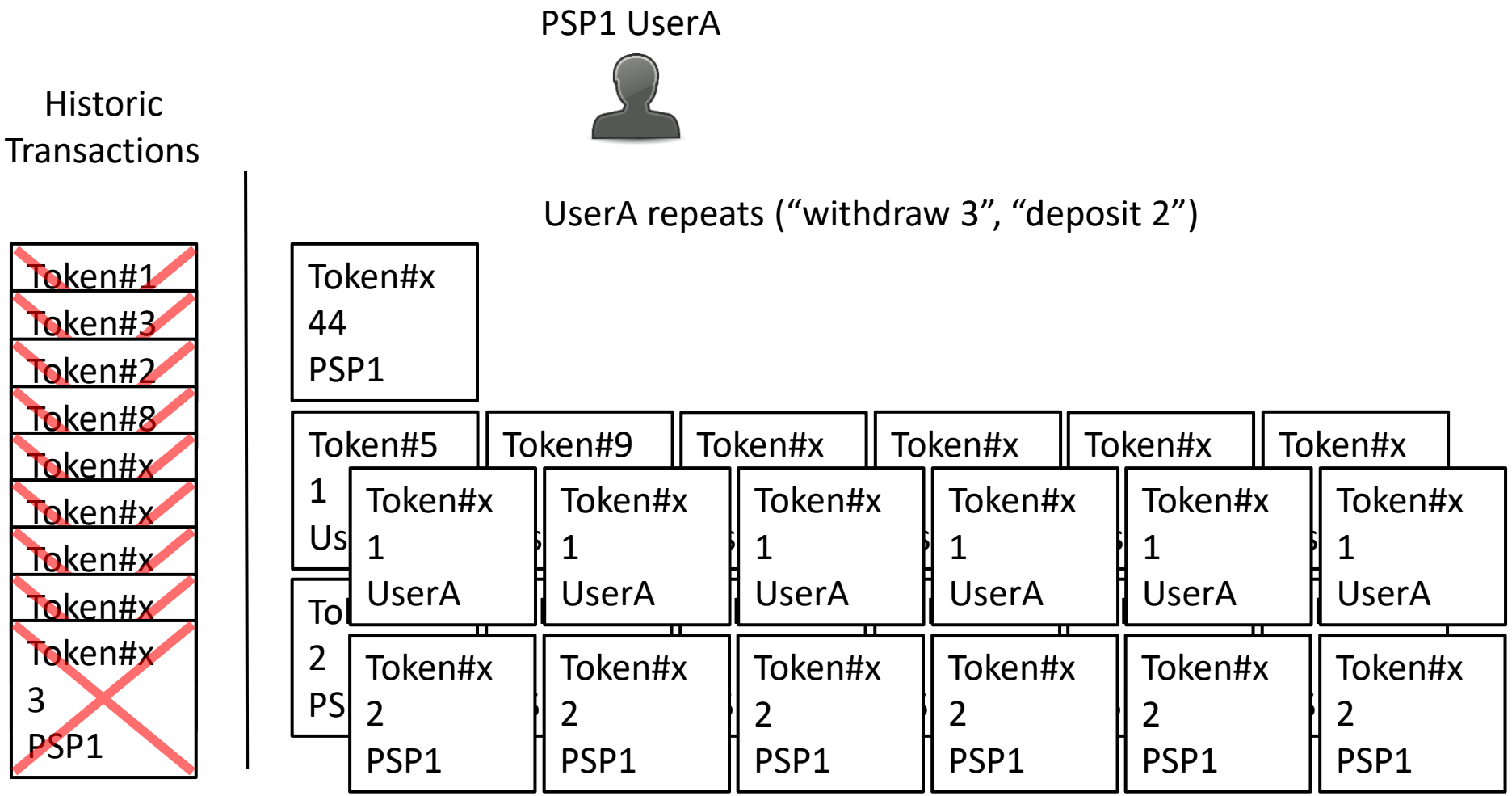
Last two years been working with everything regarding security in the project.

What is backchain and why do Corda work? And how to exploit bad implementation...

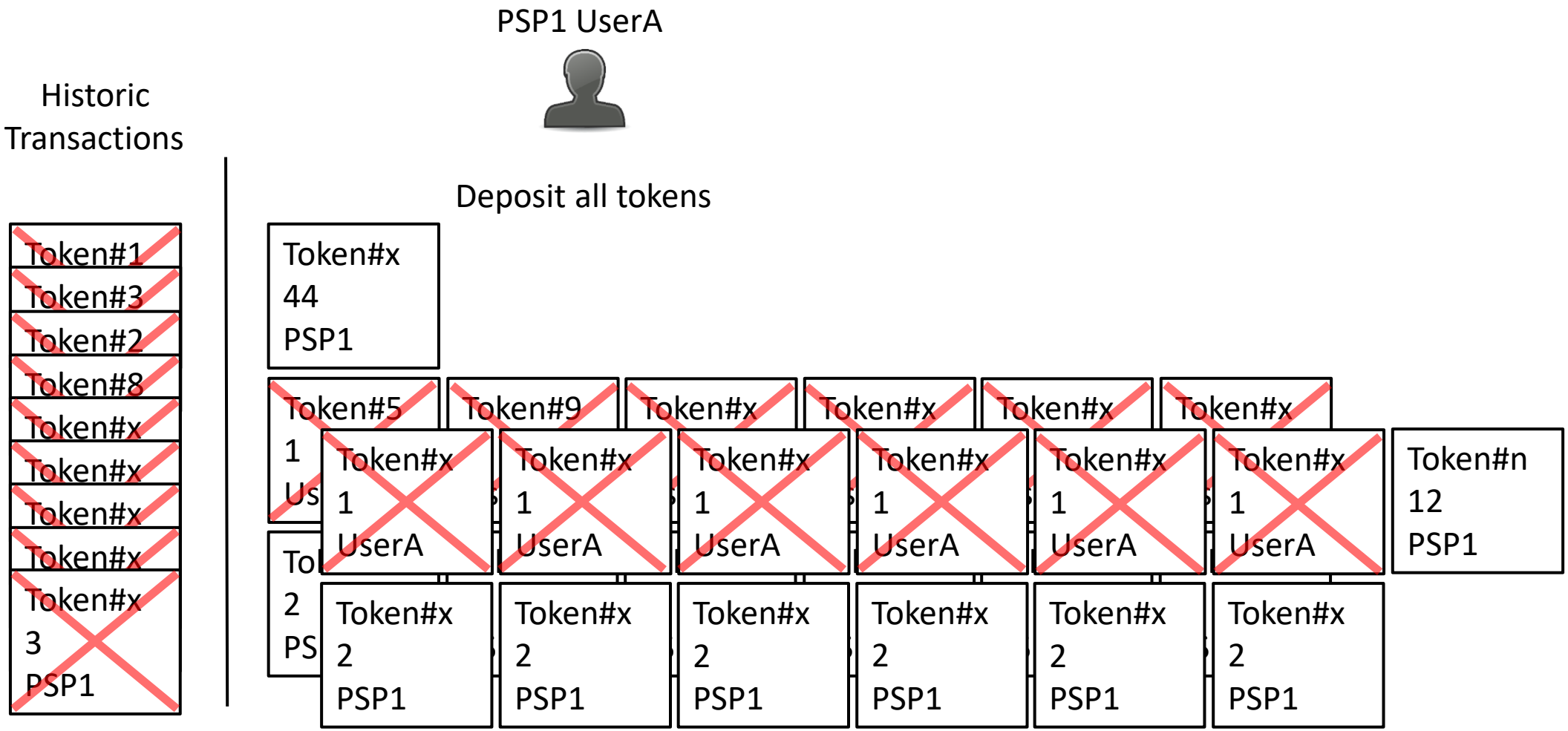




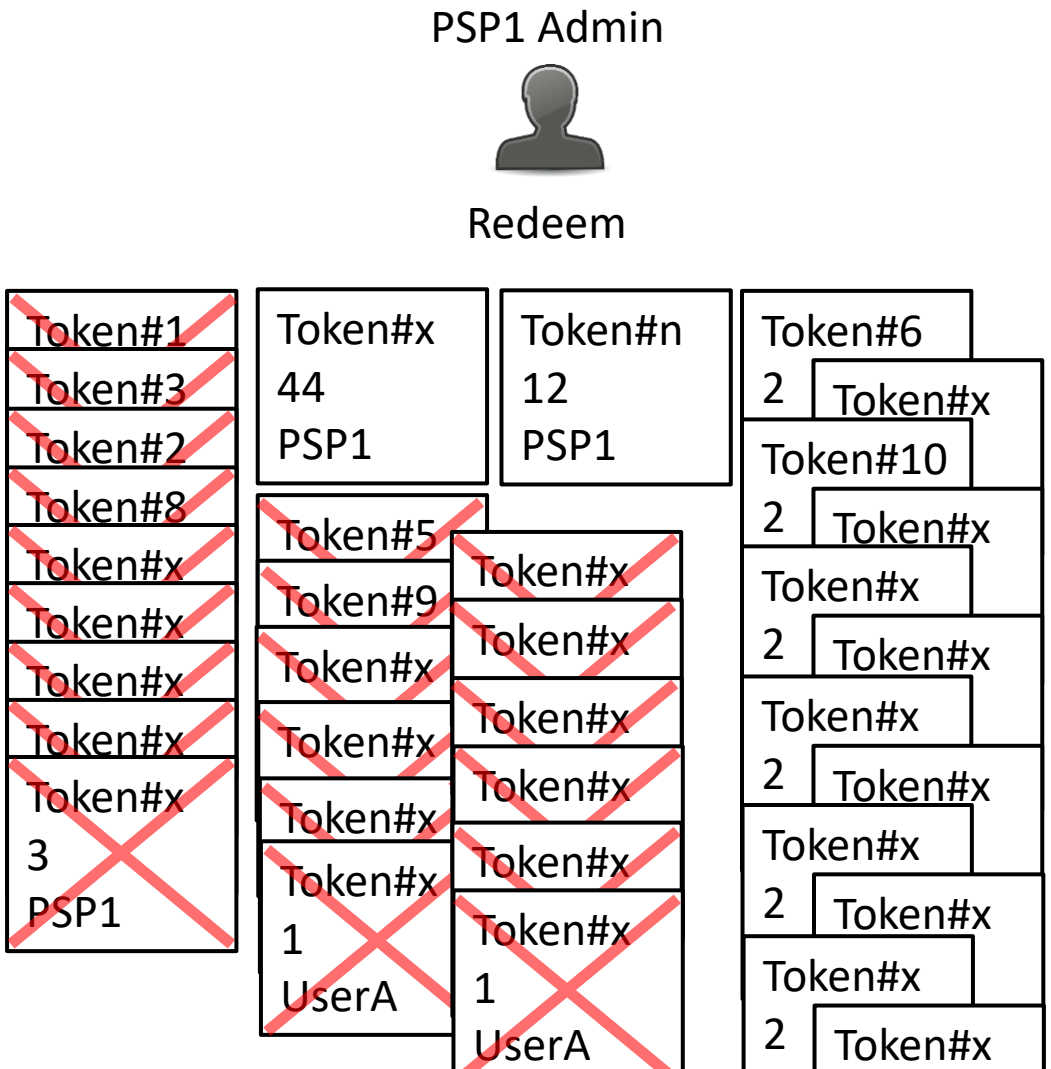
How to exploit token selection and long backchains

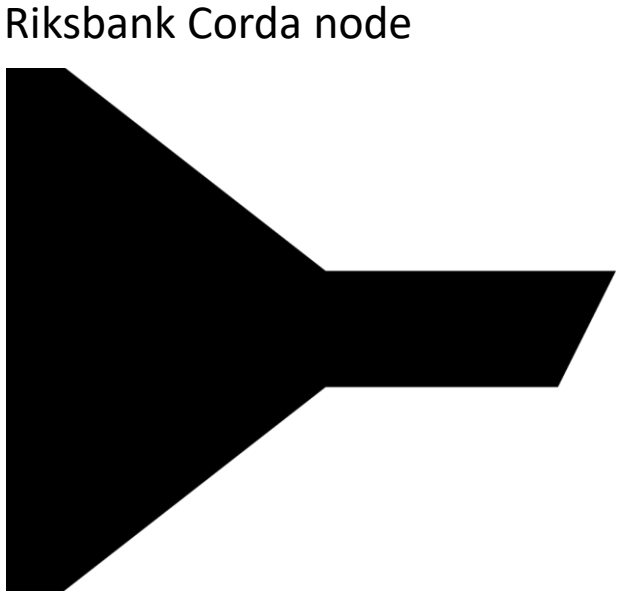


How to exploit token selection and long backchains



How to exploit token selection and long backchains



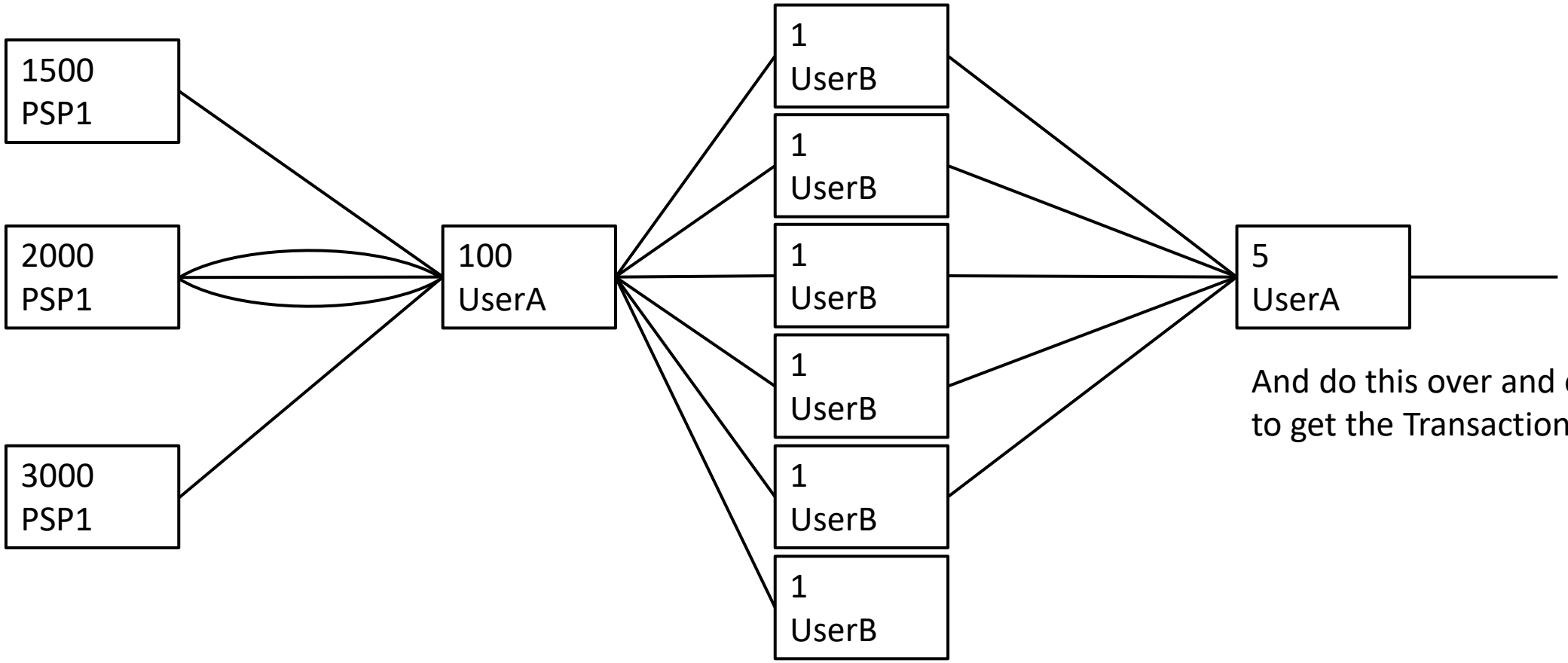


Other setups with better effects

Several issue tokens to
get several merkle trees

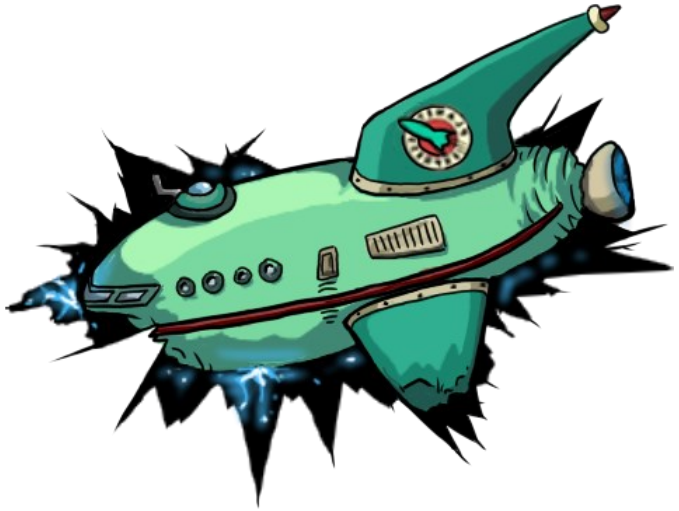
Split tokens into hundreds

Use hundreds of tokens in one transaction



And do this over and over again
to get the TransactionOfDeath

Crash nodes with TransactionOfDeath and permanently lock tokens



Sometimes crashes gives inconsistencies.

Token#1
5
UserA

UserA => UserC

Token#2
5
UserC

Available token: Token#1

PSP1
Corda
node

PSP3
Corda
node

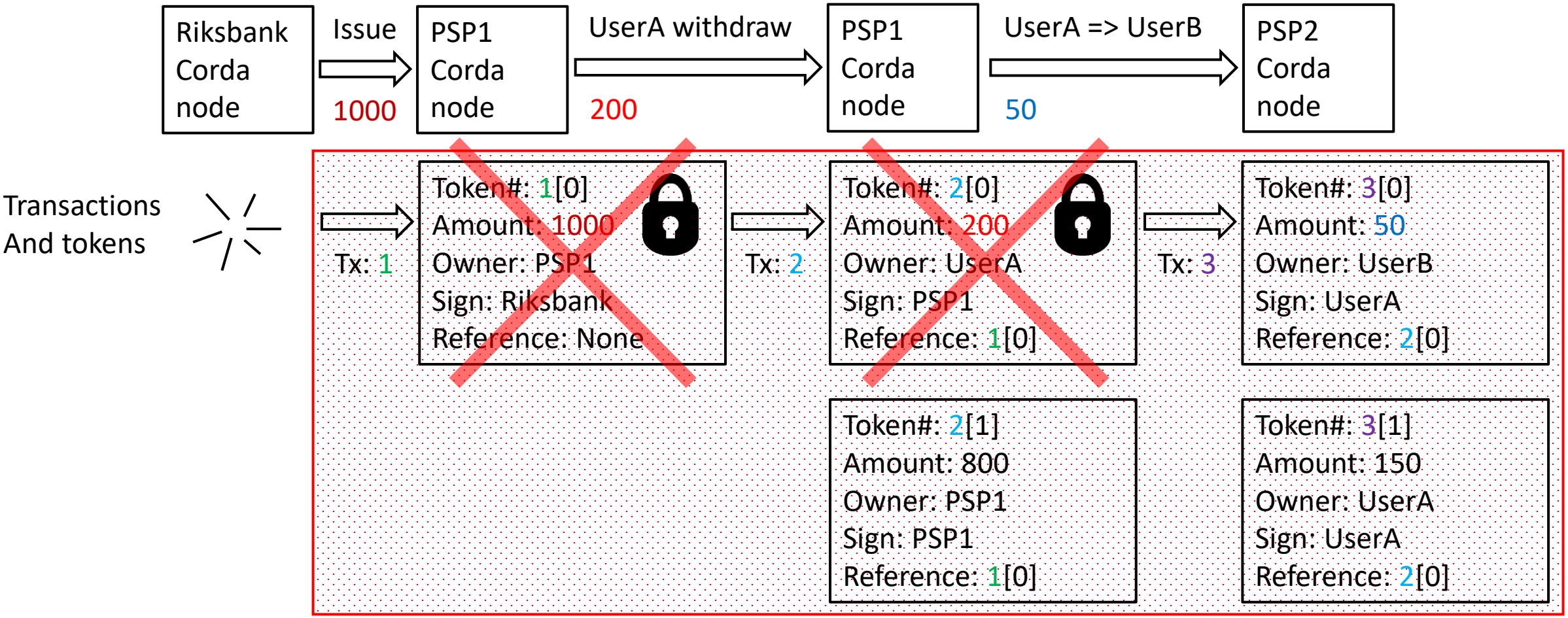
Mark Token#1 as used

Riksbank
Corda
notary

Used token: Token#1

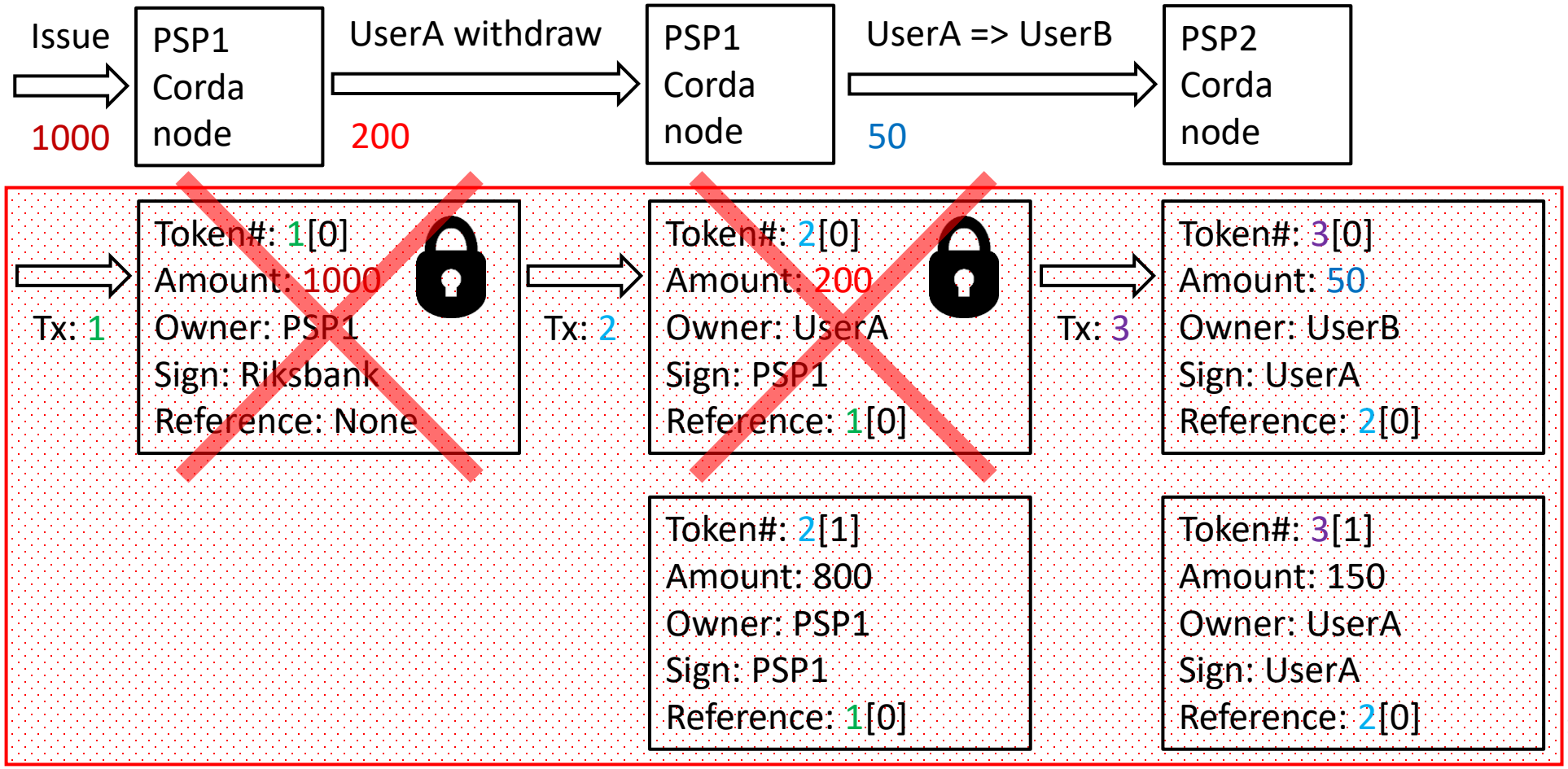
Backchain and privacy

To be able to verify authenticity of the tokens all historic transactions for that token is needed.



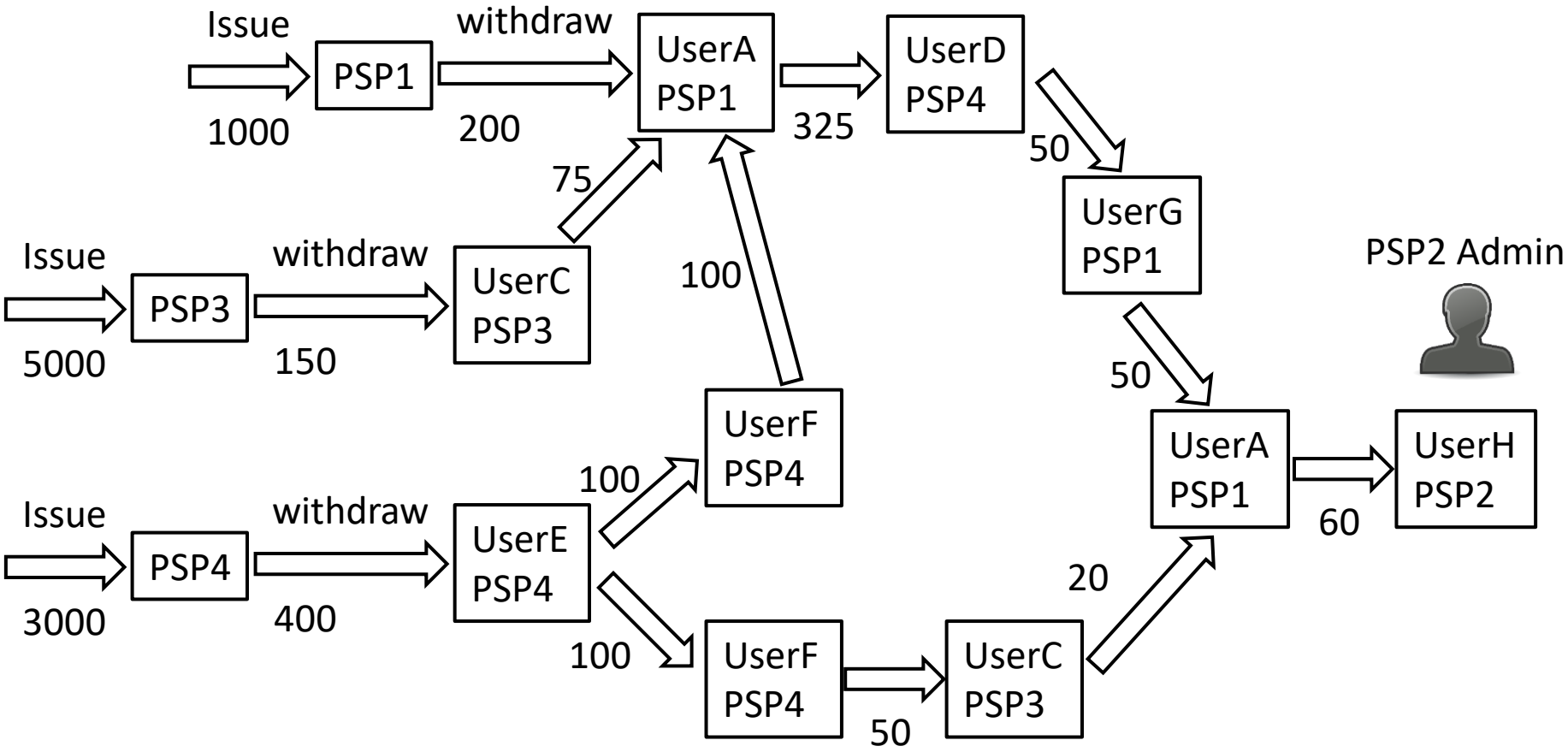
Backchain and privacy

So PSP2 can see how PSP1 have done the issue and how the UserA withdrawn 200.



Backchain and privacy

Older and longer backchains reveals more.



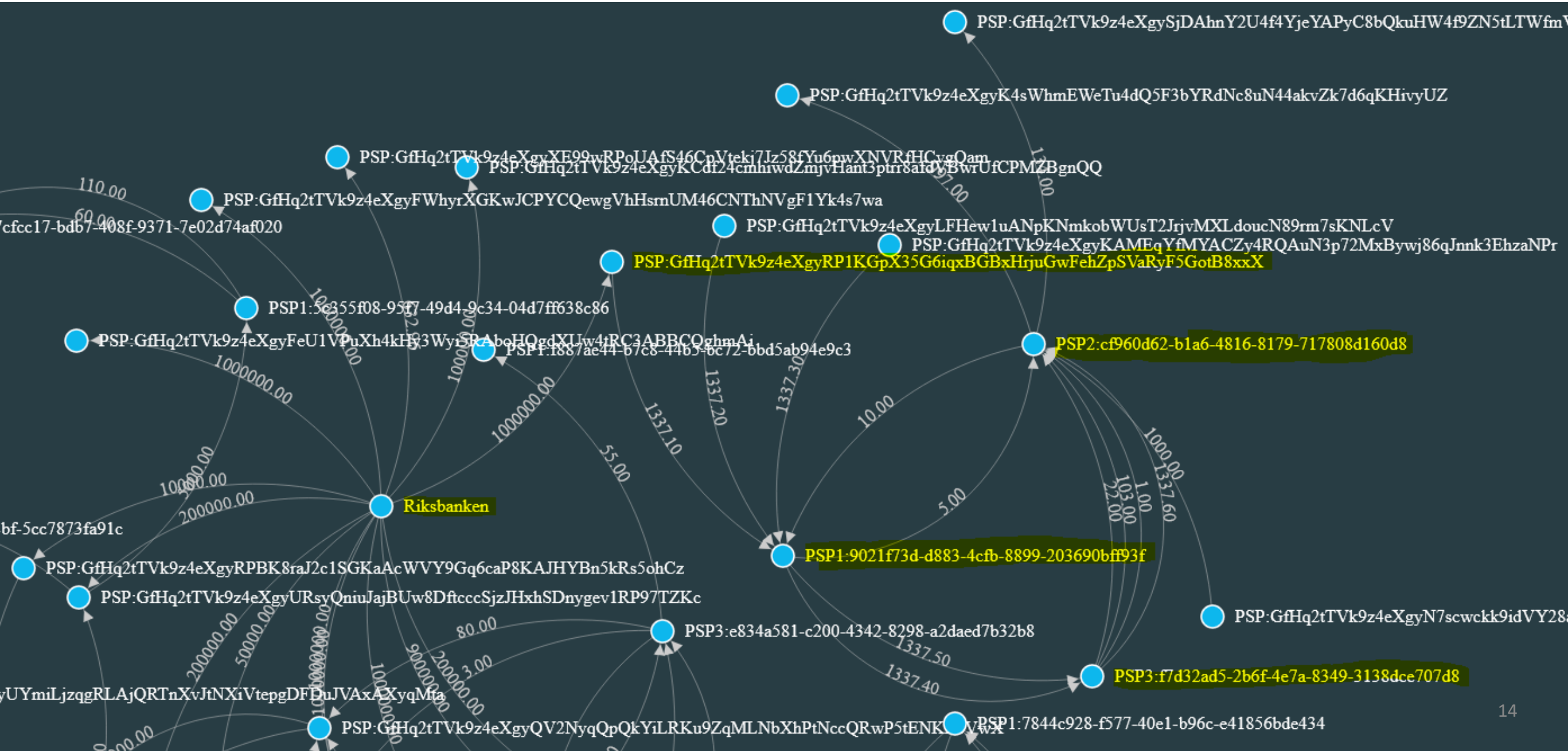
Practical example: PSP2 backchain

Admin of PSP2 has only information from the PSP2 Corda node and business layer of PSP2.

To be able to get the backchain and to visualize it PSP2 admin has to:

- Extract the backchain
- Get the transactions
- Datamine
- Visualize

Visualization with data only from PSP2



Backchain and privacy

Need to be compliant with:

- European General Data Protection Regulation (GDPR)
- Swedish bank secrecy regulation

Operational security challenges
Performance

Everything that must be solved before going in production with a token based retail CBDC

- Performance and authenticity of the digital currency.
  - Long backchains with many tokens
  - Concert scenario (50000 tokens in a wallet)

Operational security challenges
High availability and disaster recovery

Everything that must be solved before going in production with a token based retail CBDC

- High availability and in memory token selection.
  - How to do maintenance without disruption?
  - Crashes can create inconsistencies (which tokens are used?).
- Catastrophic failures and disaster recovery.
  - How to restore databases after a catastrophic failure?

Operational security challenges
Information and finance security

Everything that must be solved before going in production with a token based retail CBDC

- Information security (ISO 27000)
  - IT security (NIST, OWASP)
  - Laws, regulations and financial compliance
- Non-repudiation.
- A secure offline?

Solutions

There are many solutions for the presented challenges.

- Chain snipping, Chipping, Key rotation, Zero knowledge proof and other encryption.
- Validating notary node.
- Hardware wallets (e.g. smart cards).
- Restore procedures and functions for correcting inconsistencies.

But... The solution can impact performance and all the other requirements need to be fulfilled.

The Riksbank is now experimenting with other designs and will also look at other technologies.


Thank you for
attending

Backup Slides

Detailed system description of the prototype