Web3: A Decentralized Societal Infrastructure

for Identity, Trust, Money, and Data

J.W. Bambacht

28 Feb 2022

TU Delft

Supervisors
Dr. Ir. J.A. Pouwelse, TUDelft
A. De Kok, RvIG

Rijksdienst voor Identiteitsgegevens
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Outline

- Problems
- Usages
- Infrastructure
- Design & Implementation
- Analysis
- Platform Demo
- Conclusion

Problems

current online world

TU Delft

What are the problems in current online world?

- no self-sovereignty of identity, money, and data
- centralization
- governments own and control identities
- platforms lack authentic trust in online conversations
- big-tech platforms **store** and **sell** personal user data
- financial system expensive, unfit for cross-border, no privacy

Usages

current online world

TU Delft

What (self-sovereign) identity solutions are there?

Self-Sovereign Identity (SSI): identity that is controlled by its natural owner only

Current solution

DigiD

- authenticator
- central server
- industry-grade security
- expensive

SSI solution

IRMA

- local identity
- central server
- IRMA infrastructure
- no offline verification

SSI solution

sovrin

- permissioned blockchain
- local identity and info
- no offline verification
- central authority

local SSI

decentralization

offline-capable

TU Delft

What are the characteristics of existing platforms?

centralized						decentralized			
client-server							peer-2-peer		
end-2-end encryption			-		end-2-end encryption				
requires and stores metadata					minimal metadata, no storage				
privacy-sensitive requirements						no requirements			
private information for trust enforcement						only forgeable information for trust			

TU Delft

Infrastructure

of the platform

TU Delft

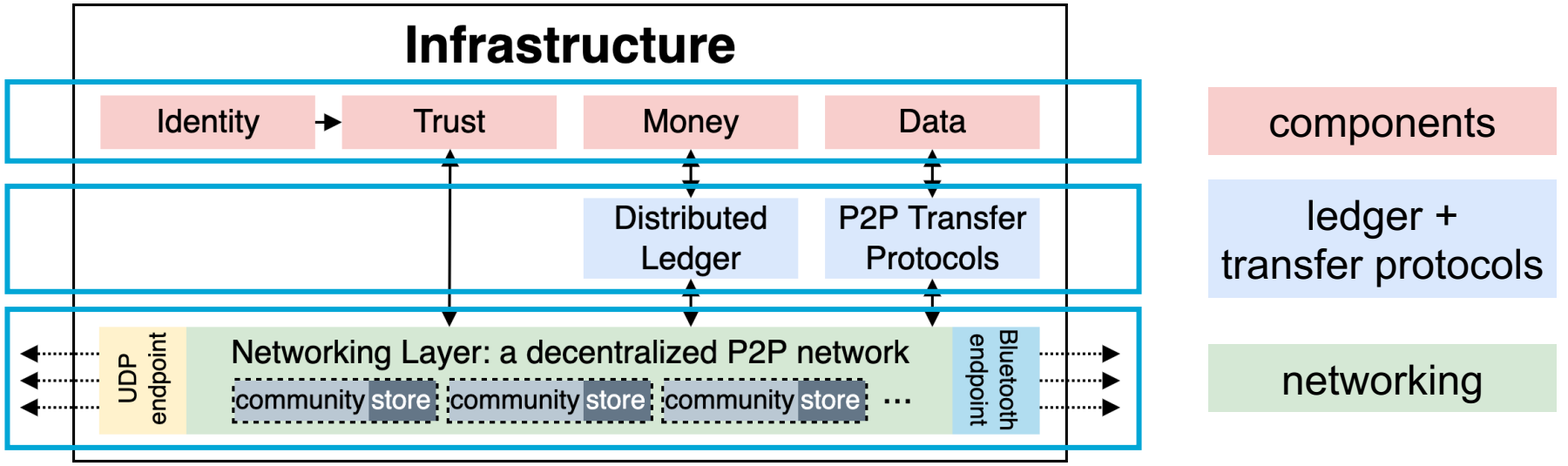
The infrastructure of our platform...

Characteristics:

- decentralized and P2P
- no storage and minimal metadata
- data confidentiality and integrity
- anonymous peer identification

Structure:

- networking layer
- distributed ledger
- data transfer protocols



TU Delft

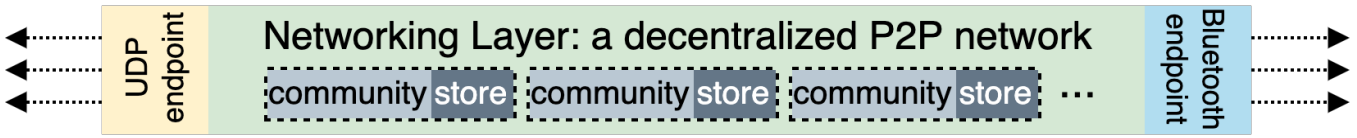
Networking layer: IPv8

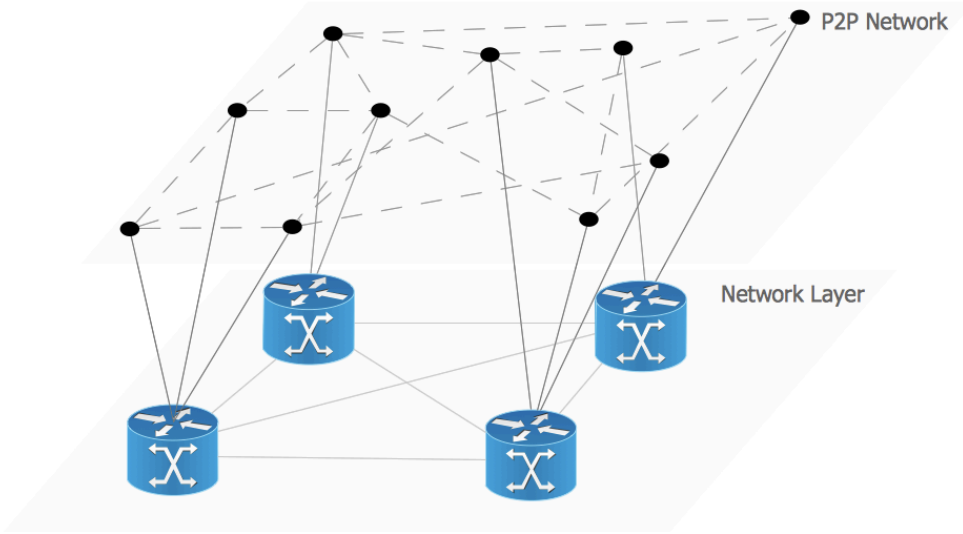
Characteristics:

- connectivity and communication
- decentralized and P2P
- zero-server infrastructure
- public-key cryptography for encryption and peer identification
- online and offline communication

Functionalities:

- network overlays / communities
- extends base layer
- community for conversations, SSI, money





TU Delft

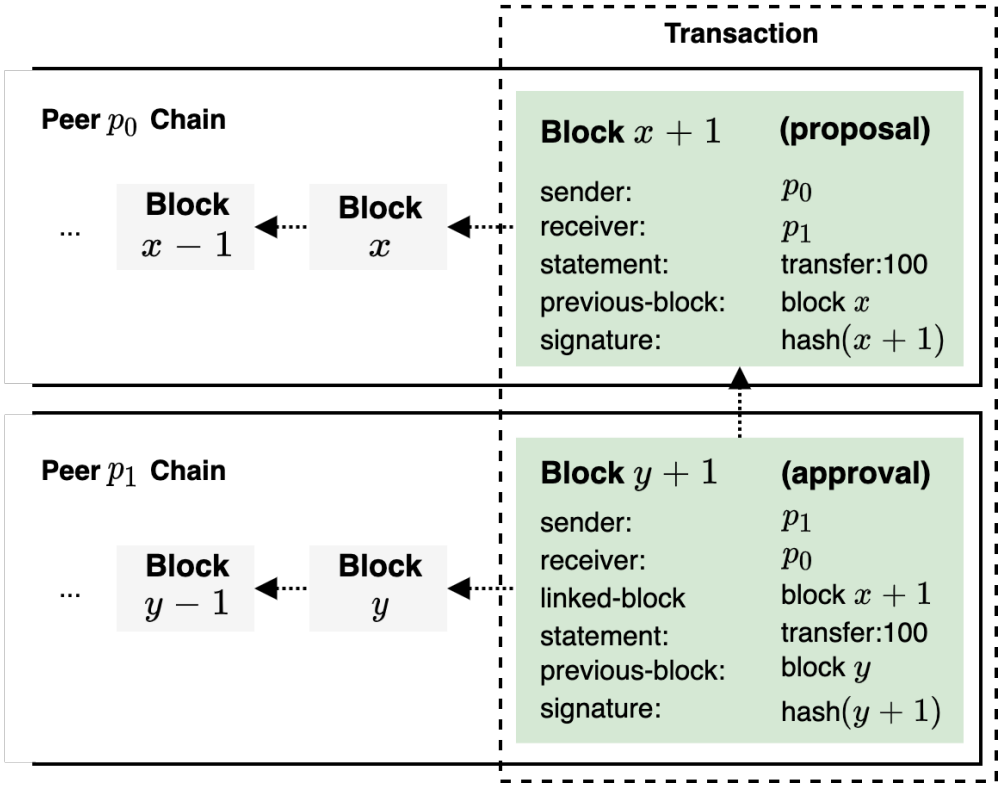
Distributed ledger: TrustChain

Characteristics:

- exchange and storage financial transactions
- permission-less and scalable blockchain
- personalized chain for each peer

Functionalities:

- send and receive blocks
- transaction = proposal + approval block
- transparent and pseudo-anonymous



TU Delft

Design & Implementation

of the platform

TU Delft

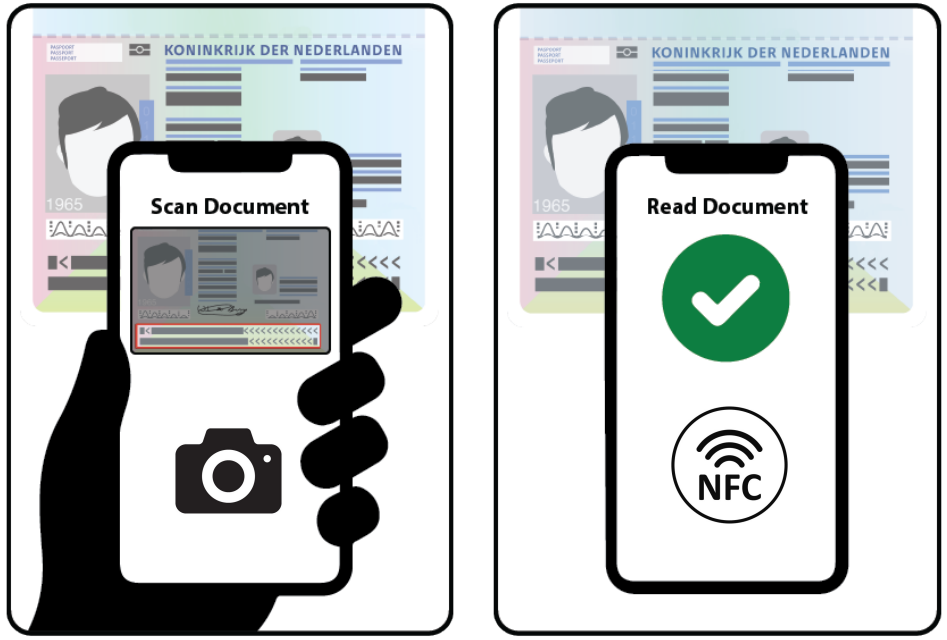
Self-Sovereign Identity (SSI) in our platform

Characteristics:

- authentic base for self-sovereignty
- authentication using local SSI
- private verifiable claims using identity attestations
- storage of validated diplomas, (COVID) certificates, …

How to get the self-sovereign identity?

- citizens possess passport or ID card
- identity in MRZ and biometric chip
- both required for authentic SSI
- scan MRZ with camera and AI
- read biometric chip with NFC

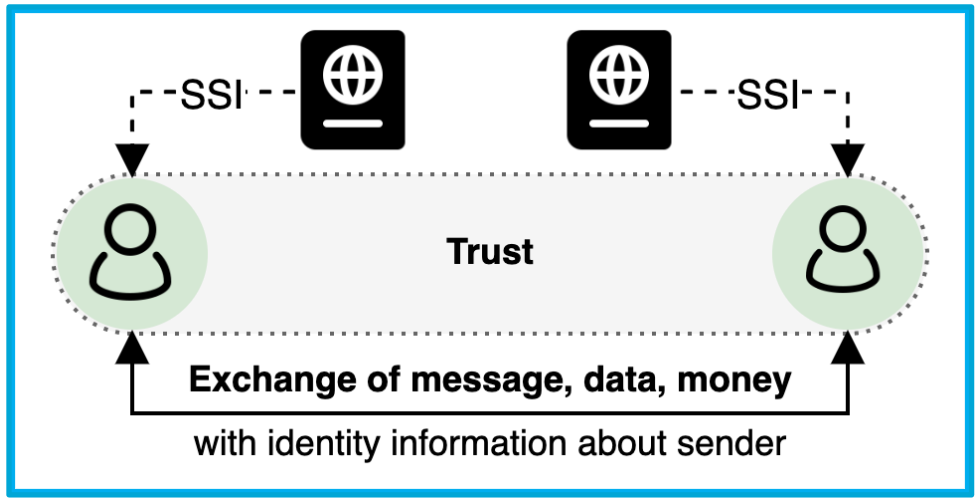


TU Delft

Enforcement of trust in our platform

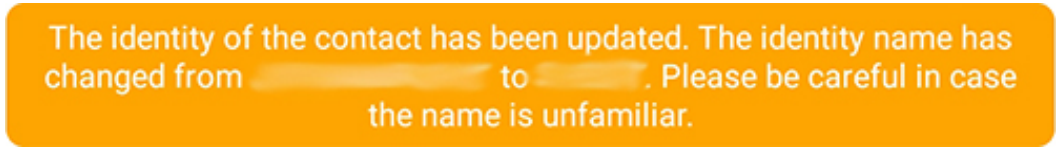
Characteristics:

- trust in platform with decentralization
- trade-off between privacy and trust
- trust using authentic information
- attributes from self-sovereign identity



How to enforce authentic trust?

- formal identity behind every sent message
- exchange identity information attributes:
  - initials + last name (**J.W. Bambacht**)
  - identity photo
  - verification status (**verified/unverified)**
- detection for changes in formal identity



Exchange of money in our platform

Characteristics:

- Central Bank Digital Currencies (CBDC)
- digital native currency on blockchain
- fast and cheap cross-border exchange
- transparent but still pseudo-anonymous
- no external dependence

How do we use this CBDC?

- EuroToken with TrustChain ledger and IPv8
- private P2P exchange
- EuroToken balance in wallet
- exchange portal for exchange of € and tokens
- Tikkie-like payment requests

TU Delft

Exchange of data in our platform

Default IPv8 data transfer protocol:

- fast for messages and small data
- UDP packet delivery is unreliable
- limited in performance
- no delivery guarantees

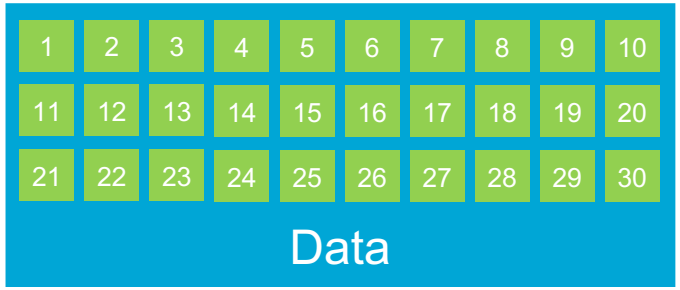
need for a reliable P2P data transfer protocol for large data

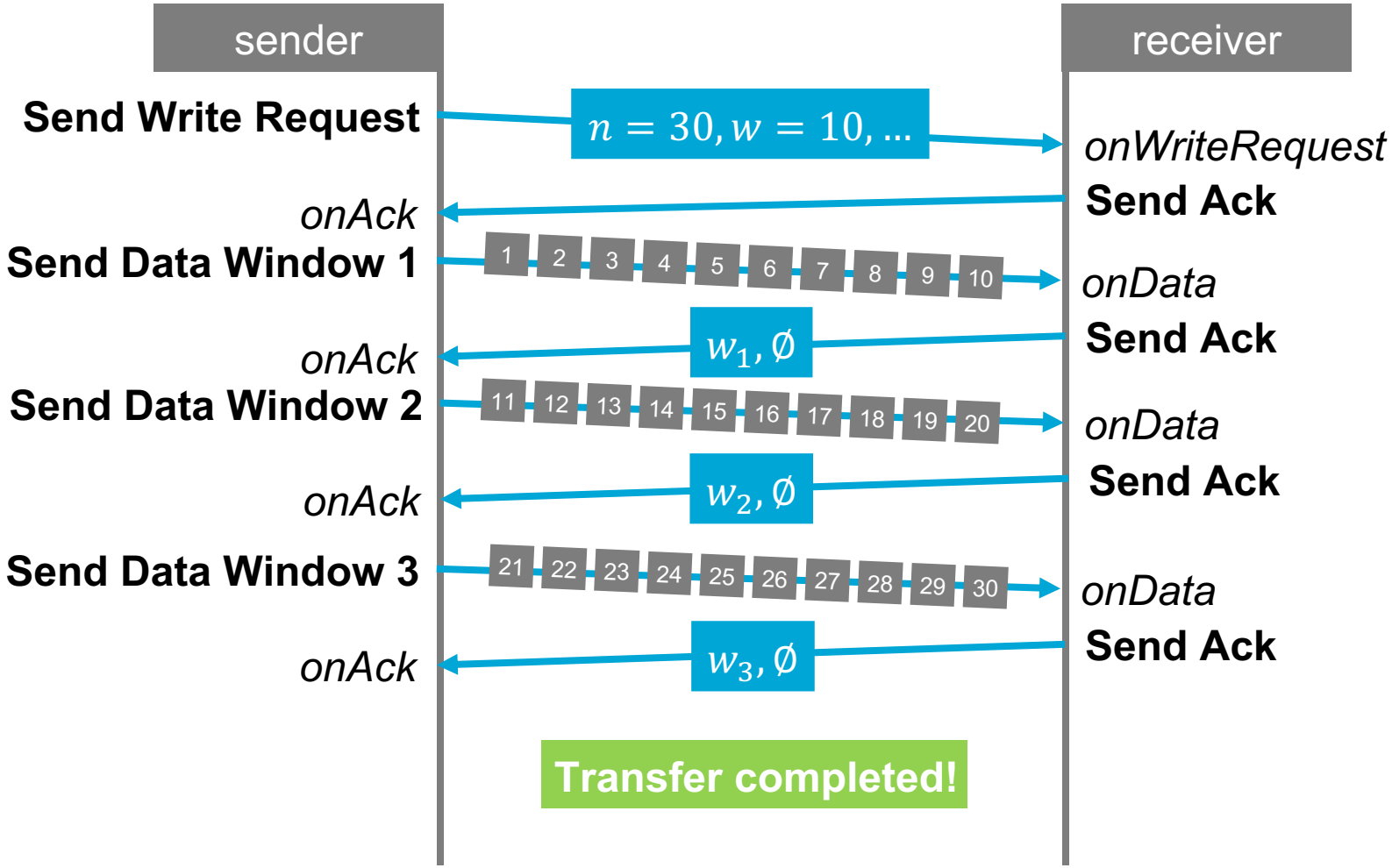
How to exchange large data?

- reliable and optimal performance
- based on principles of TFTP
- authenticated and encrypted
- acknowledgement-based
- windowing for performance increase
- progressive delivery guarantees
- adaptive downscaling of performance

Normal operation of data transfer protocol

Data of $n = 30$ blocks and window of $w = 10$ blocks

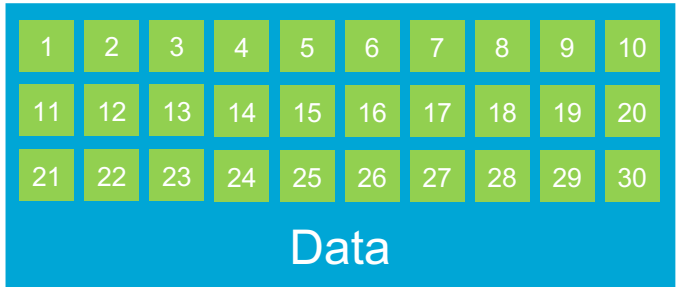


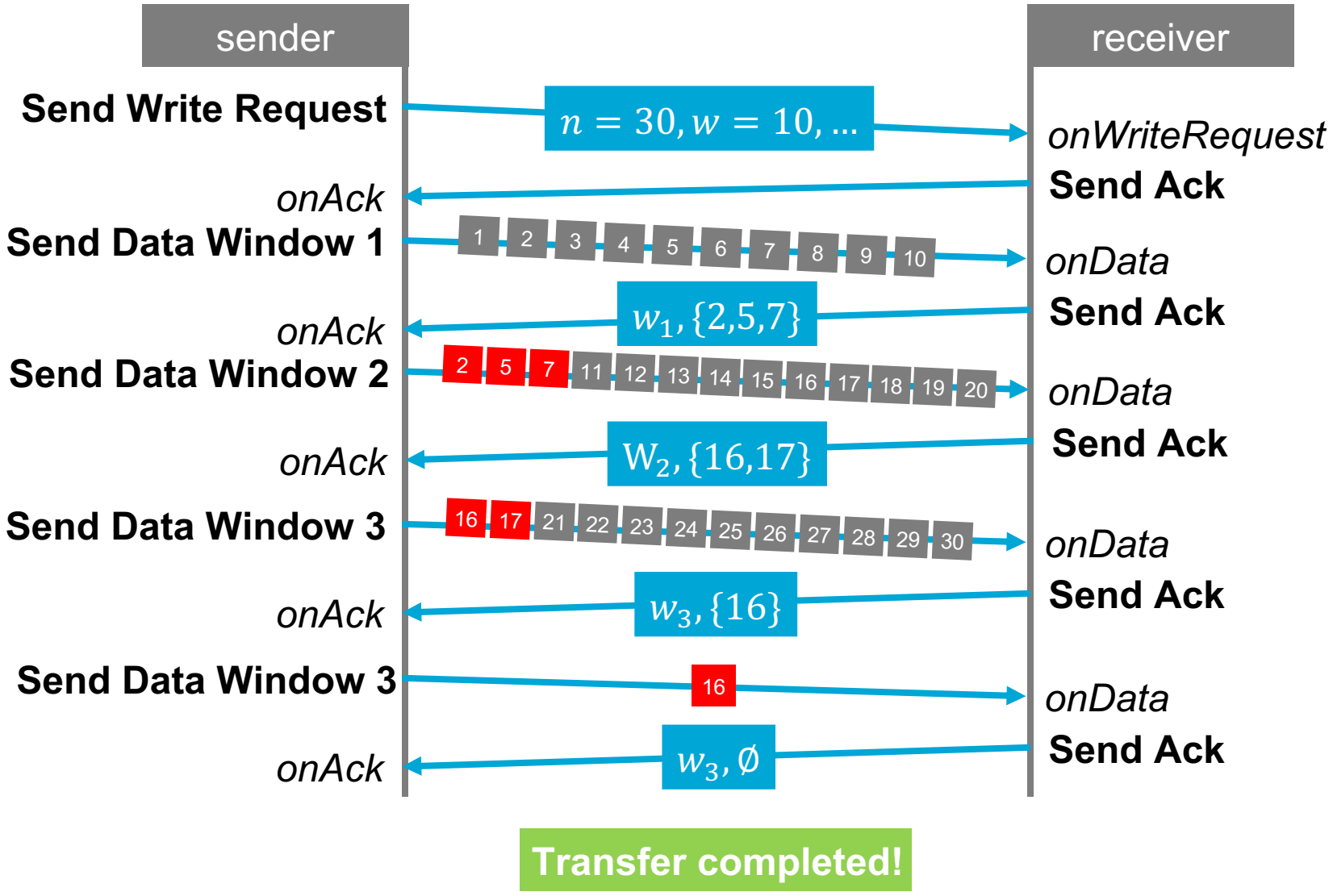


TU Delft

Progressively continue normal operation with packet loss

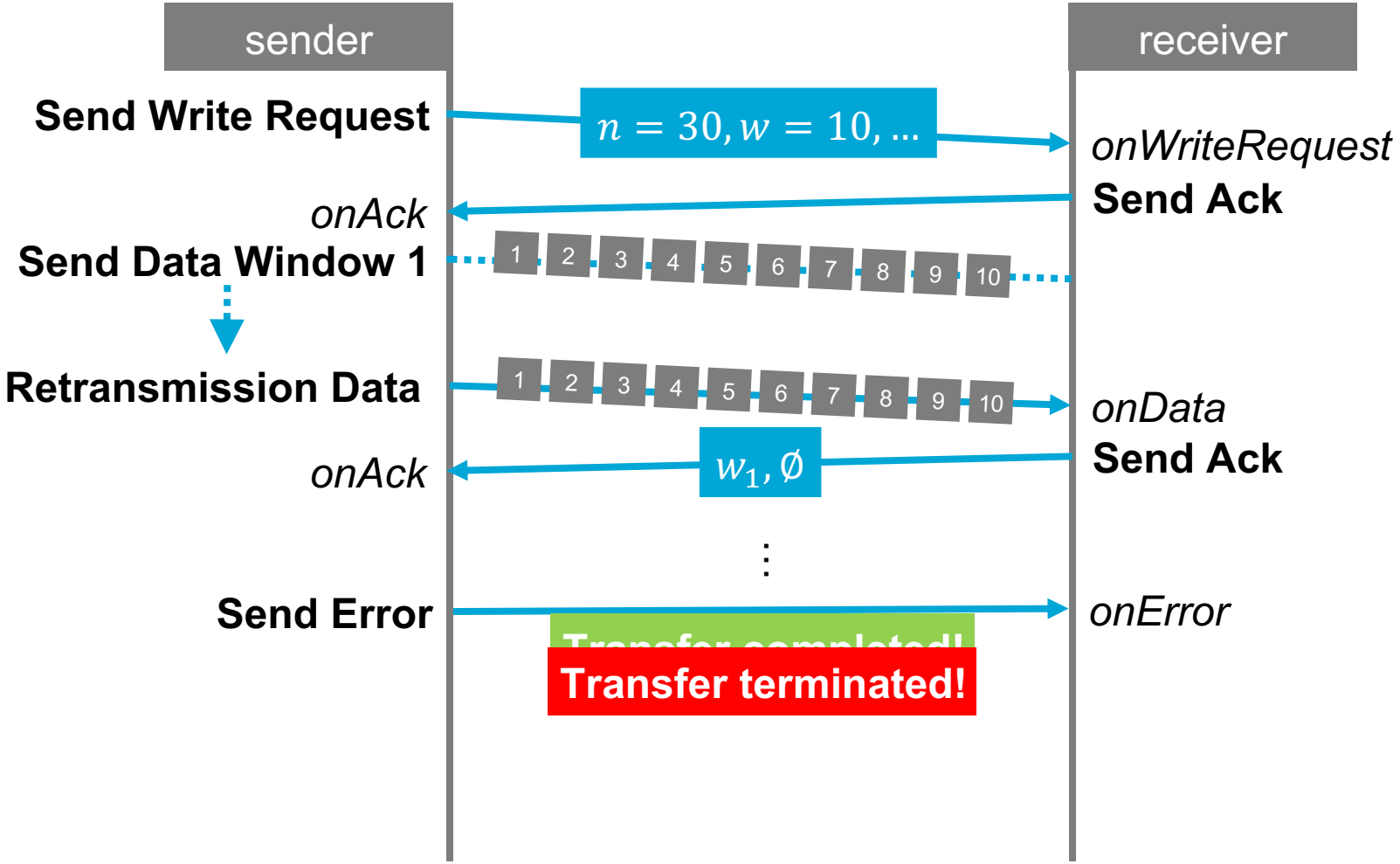
Data of $n = 30$ blocks and window of $w = 10$ blocks





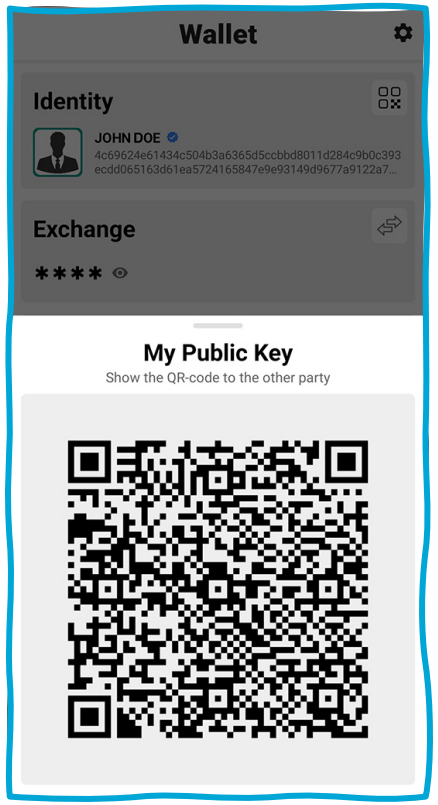
TU Delft

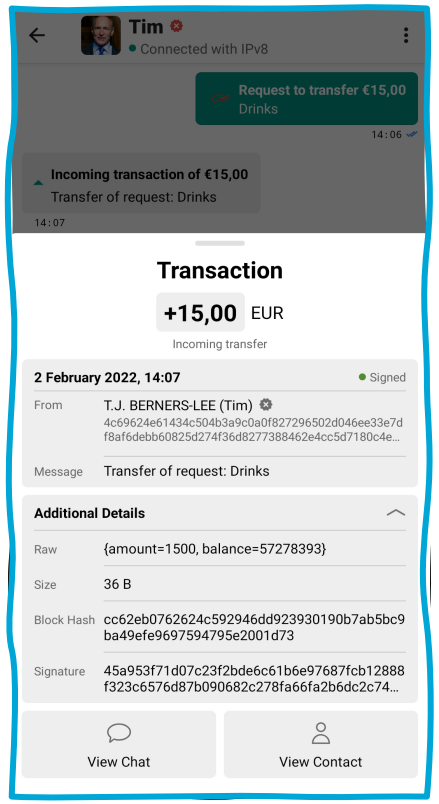
Retransmission and error

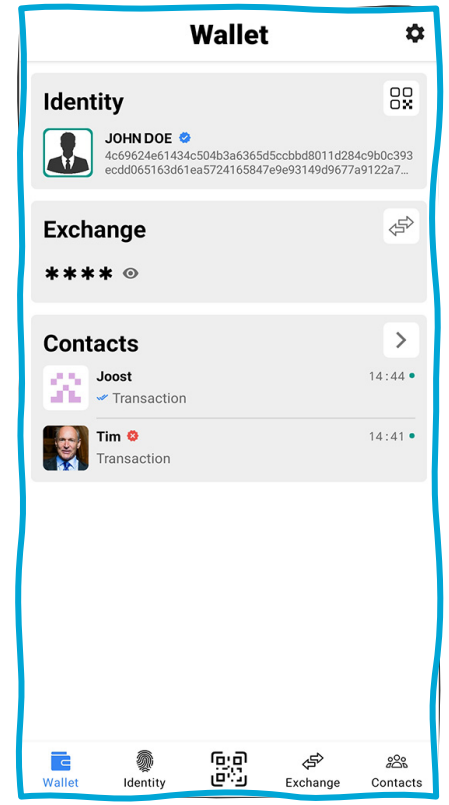


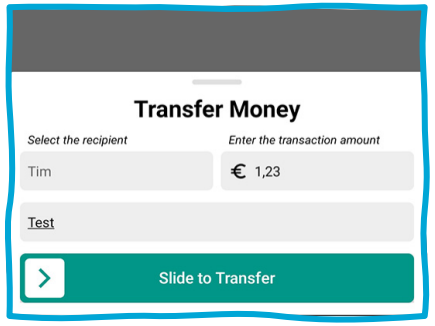
UX and UI Design

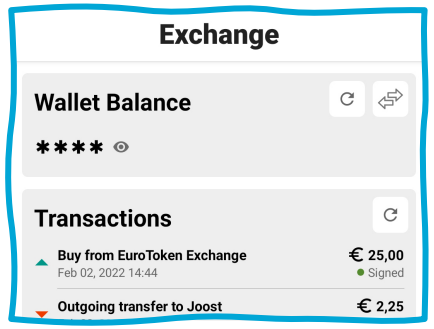
- user experience and layout
- simple and consistent design
- master-detail interface
- QR-codes
- protection mechanisms
- download status

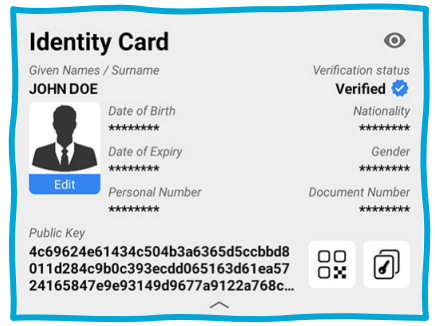


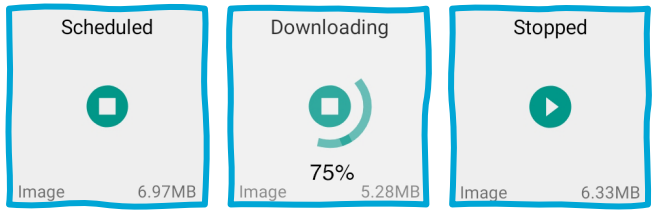












TU Delft

Analysis

data transfer protocol

TU Delft

Experimental analysis of data transfer protocol

Analysis:

- optimal parameters for **normal** operation:
  - I. max transfer speed
  - II. min lost packets
  - III. min retransmissions
- ideal situation, no latency, no packet loss
- optimize block size B and window size W

Setup:

- 2 Android phones
- local WiFi network
- $B = \{600, 700, 800, 900, 1000, 1100, 1200\}$ bytes
- $W = \{16, 32, 48, 64, 80, 96, 112, 128\}$ blocks
- 5 iterations
- 2 file sizes

TU Delft

Experimental results of data transfer protocol

Observations:

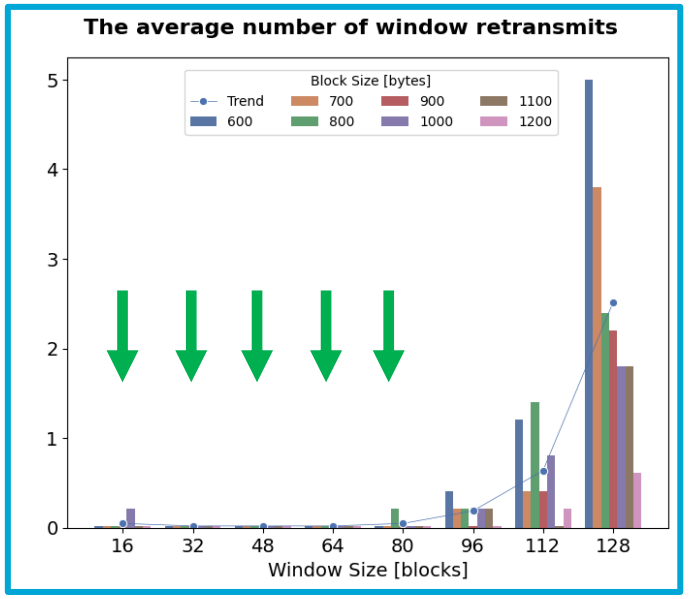
I. maximal transfer speed:
   - B: higher size = higher speed → 1200 bytes
   - W: 80 or 96 blocks optimum

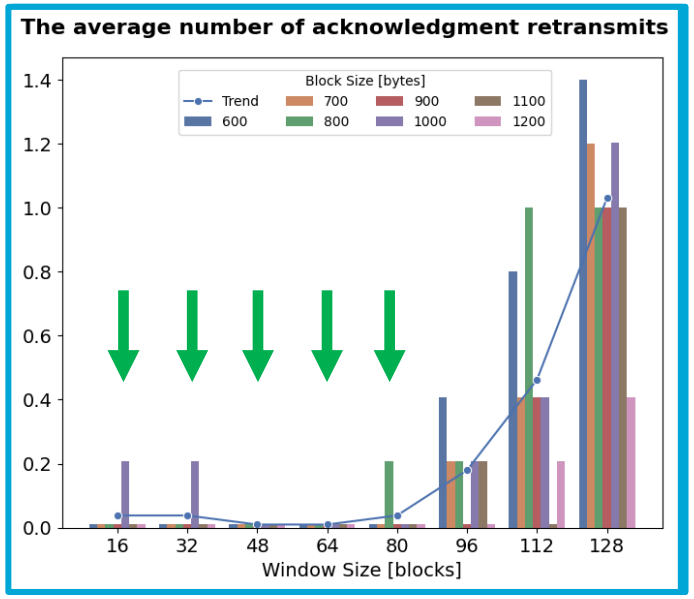
II. minimum lost packets:
   - B: no optimum
   - W: 80 or **96** blocks optimum

III. minimum retransmissions:
   - B: no optimum
   - W: <96 blocks optimum

What can we conclude?

- optimal block size B of 1200 bytes
- optimal window size W for 80 blocks
- independent on file size





TU Delft

Platform Demo

Conclusion

TU Delft

What can we conclude?

- no self-sovereignty with centralization
- decentralization ⇏ self-sovereignty
- P2P for privacy and security
- reliable, private and secure P2P data transfer protocol
- first Self-Sovereign Identity in social platform
- authentication, attestations, trust enforcement, …
- private exchange euro Central Bank Digital Currency euro

BIG-TECH COMPANIES, GOVERNMENTS, AND BANKS NEED TO STEP UP FOR SELF-SOVEREIGNTY!

TU Delft

Questions?

TU Delft

Sources

- Roig, M. (2021). Photograph on cover from https://www.paymentsjournal.com/can-banks-acquire-customers-with-biometric-payment-cards/
- Clarke, P. (2014) Photograph of Tim Berners Lee in screenshots from https://commons.wikimedia.org/wiki/File:Sir_Tim_Berners-Lee_(cropped).jpg
- Overlay network ConceptDraw Solutions from https://conceptdraw.com/How-To-Guide/overlay-network
- DigiD logo from https://www.digid.nl
- IRMA logo from https://privacybydesign.foundation
- Sovrin logo from https://sovrin.org
- WhatsApp logo from https://commons.wikimedia.org/wiki/File:WhatsApp.svg
- Facebook Messenger logo from https://nl.m.wikipedia.org/wiki/Bestand:Facebook_Messenger_logo_2020.svg
- Telegram logo from https://commons.wikimedia.org/wiki/File:Telegram_logo.svg
- iMessage logo from https://commons.wikimedia.org/wiki/File:IMessage_icon.png
- WeChat logo from https://seeklogo.com/vector-logo/284905/wechat
- Signal Messenger logo from https://commons.wikimedia.org/wiki/File:Signal-Logo.svg
- Session Messenger logo from https://commons.wikimedia.org/wiki/File:Логотип_Session_messenger.png
- Status.im logo from https://status.im
- Sylo logo from https://sylo.io/wallet/press-kit/
- Berty logo from https://berty.tech

TU Delft