DEUTSCHE BUNDESBANK EUROSYSTEM

Crypto Oversight in the Euro Area Based on the PISA Framework – Some Preliminary Thoughts on "Decentralised" Payment Schemes

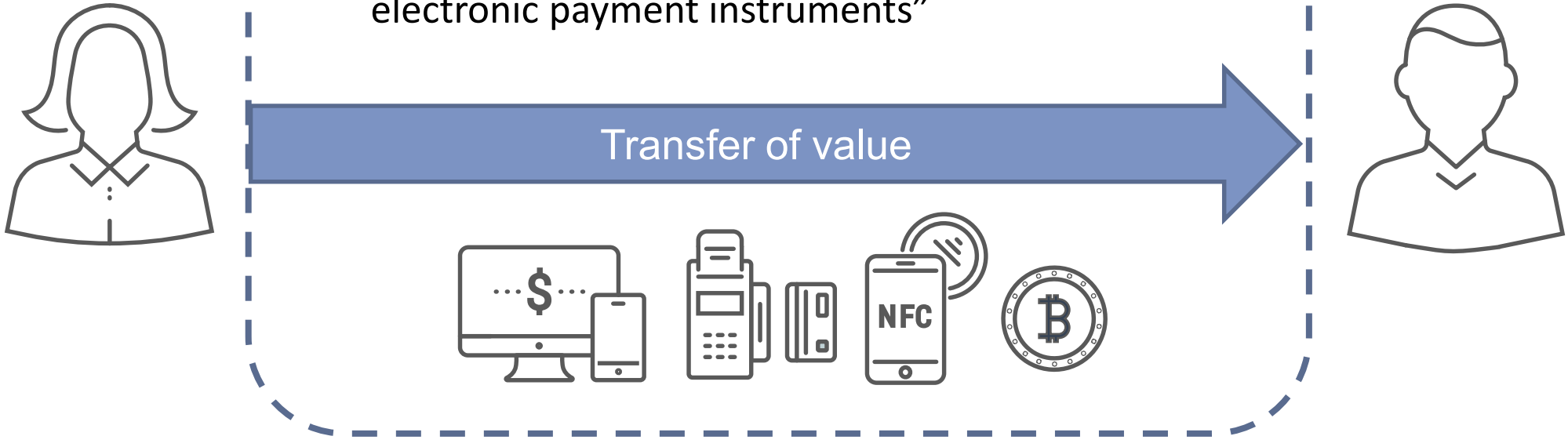
Stefan Mitzlaff, Payment System Analysis, Deutsche Bundesbank

Oversight Framework
Overview

- Eurosystem oversight framework for electronic payment instruments, schemes and arrangements (PISA); (effective from 1 November 2022)
  - Covers schemes and arrangements based on general purpose electronic payment instruments
  - Focus on schemes/arrangements that play a significant role in the euro area
  - Complements the oversight of individual payment systems and critical service providers

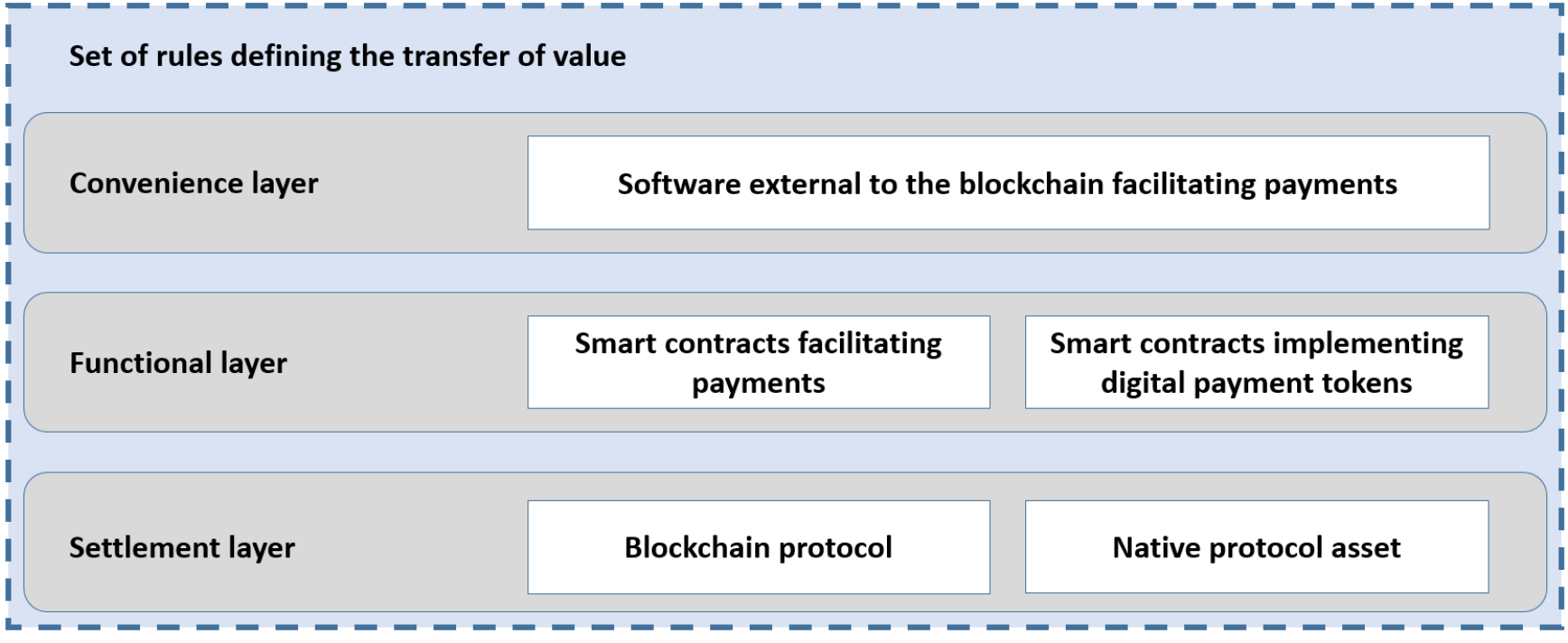
PISA Framework
Stylized Payment Scheme

- Payment scheme: “set of (…) rules enabling the transfer of value between end users by means of electronic payment instruments”



PISA Framework
Non-Scope – “Decentralised” Payment Scheme

Figure: Stylised stack of a decentralised payment scheme



Source: Own illustration.

PISA Framework
Scope – Oversight Process of "Centralised" Payment Schemes

"Centralised" governance body:
- "legal entity, part of a legal entity, or several legal entities"
- Defines "set of rules enabling the transfer of value"

1 Collect data/information

Tasks payment oversight:
- Checks oversight-relevance
- Makes actual assessment

2

3 Assessment

Governance body:
- Implementation of oversight recommendations (e.g. risk mitigating measures)

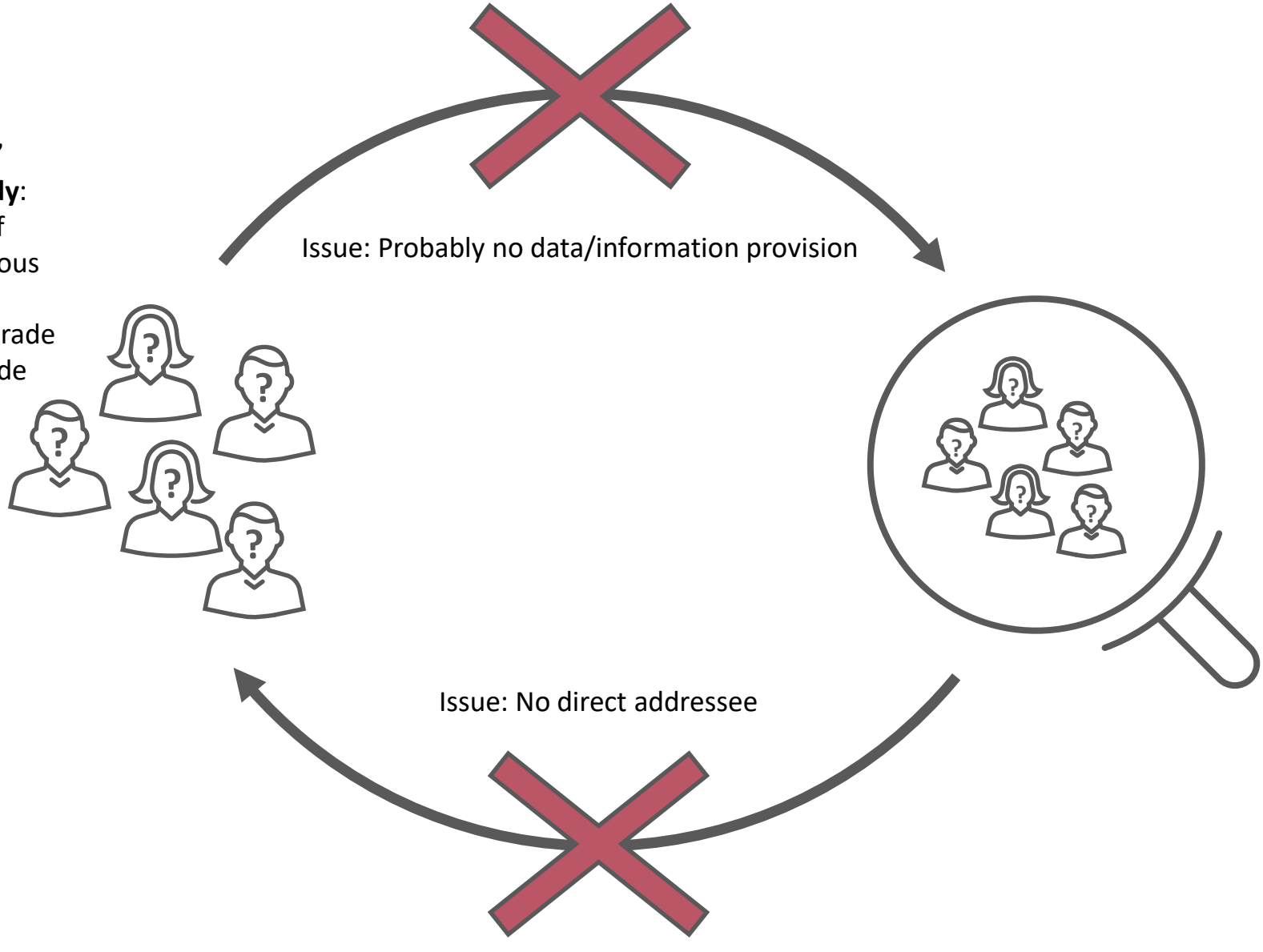
4

PISA Framework

Non-Scope – Potential Oversight Process of “Decentralised” Payment Schemes

“Decentralised” governance body:

- Collective of pseudonymous participants
- Update/upgrade software code



“Decentralised” Payment Schemes
Alternative Approach

1

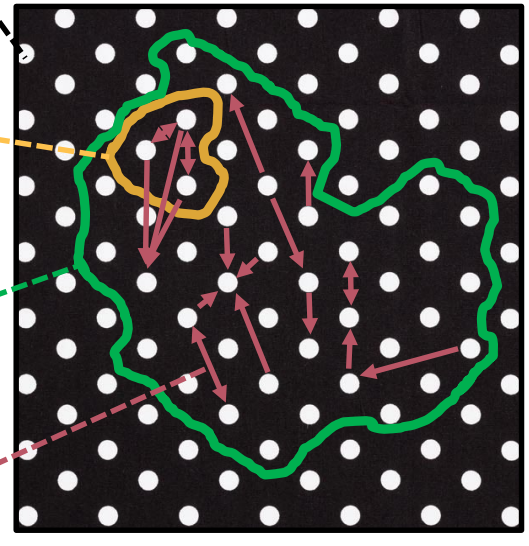
(i) De-anonymise publicly available data, and
(ii) analyse open-source software code

Tasks payment oversight:
- Checks oversight-relevance
- Makes actual assessment

2

Single wallet address

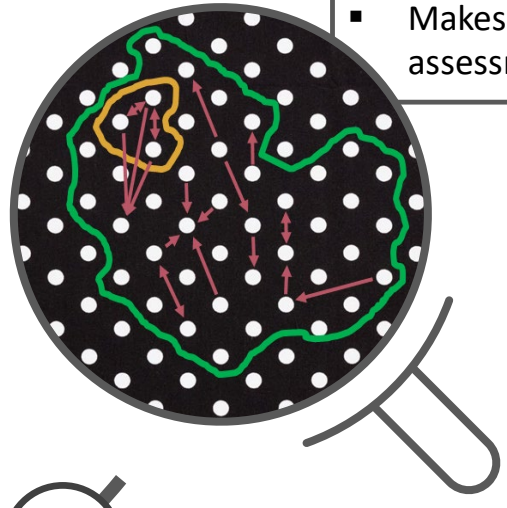
Public ledger data



Forming single user clusters

Quasi-identify euro area users

Identify payment transactions



3

Alternative addressees, e.g.:
- Merchants
- Retail customers
- Policy makers

“Decentralised” Payment Schemes – Check Oversight-Relevance

1. Step: Forming Single User Clusters

- Note: Technical peculiarities of the underlying infrastructure must be taken into account, which is why there could be no universal approach.

Potential de-anonymization techniques

UTXO-based blockchains

- Multiple input heuristic (Reid and Harrigan (2012))
  - Initiator of a transaction with multiple inputs owns all of the input addresses
- Change heuristic (Meiklejohn et al. (2013))
  - Change address created by a transaction is likely controlled by the same entity that initiated the transaction

Account-based blockchains

- Deposit address reuse heuristic (Victor (2020))
  - Deposit addresses that are created per customer by crypto exchanges are used to link different addresses that send funds to these deposit address to the same entity

“Decentralised” Payment Schemes – Check Oversight-Relevance

2. Step: Geographic Assignment of Users

Potential de-anonymization techniques

- DuPont and Squicciarini (2015) and Béres et al. (2021): Daily activity patterns could give an indication of geographic location (time zone)
  - Exceptions, e.g. night-shift workers
  - Further translation of time zones into countries in Europe perhaps on the basis of differences in the time zone implementation across countries

Currently observing CEST.
Areas with same time currently (UTC +2).

Currently observing CET.
Observes CET part of the year.
Areas with same time currently (UTC +1).

Source: www.timeanddate.com.

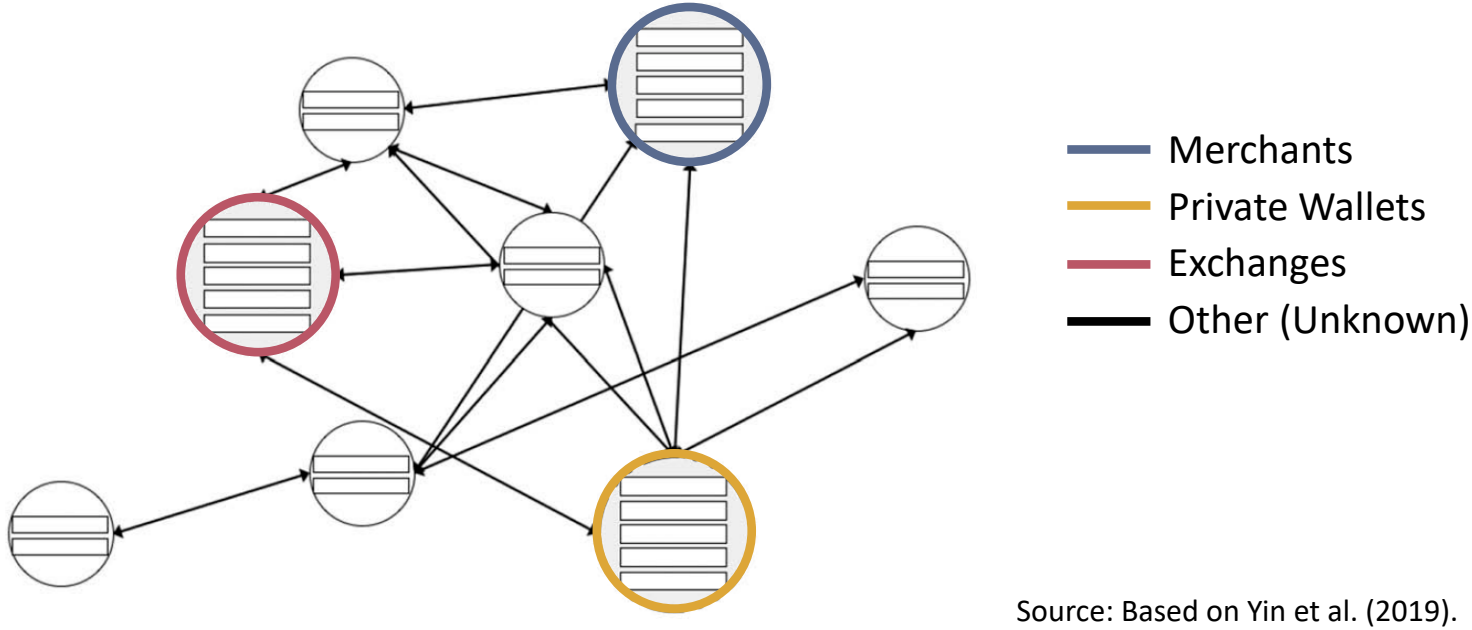
“Decentralised” Payment Schemes – Check Oversight-Relevance

3. Step: Determine Transaction Purpose

Potential de-anonymization technique

- Yin et al. (2019): Supervised machine learning algorithm to predict activity categories of users
  - Identified users (a sample of 957 entities) were used as a training set, and classifiers were built to differentiate users among twelve categories
  - Potentially oversight-relevant transactions could then for example occur between or within certain user groups such as “Merchants” and “Private Wallets”.

Figure: Network of potentially oversight-relevant user categories



Source: Based on Yin et al. (2019).

Conclusion

- “Decentralised” payment schemes …
  - are not within the scope of PISA,
  - but could be alternatively checked for oversight-relevance with de-anonymization techniques of public ledger data,
    - although (1) there could be no universal approach taking into account the technical peculiarities of the underlying infrastructures, (2) the current techniques only provide “guesstimates” for the data needed
  - could be alternatively assessed with publicly available information,
  - although they currently have no practical relevance in payments anyway – but that might change in the future.

Stefan Mitzlaff
E-Mail: Stefan.Mitzlaff@Bundesbank.de

Literature

- Béres, Ferenc, István A. Seres, András A. Benczúr and Mikerah Quintyne-Collins (2021): Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users, 2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), 2021, pp. 69-78, DOI: 10.1109/DAPPS52256.2021.00013.
- DuPont, Jules and Anna Cinzia Squicciarini (2015): Toward De-Anonymizing Bitcoin by Mapping Users Location, in: Proceedings of the 5th ACM Conference on Data and Applica-tion Security and Privacy (CODASPY '15) Association for Computing Machinery, New York, NY, USA, 139–141. https://doi.org/10.1145/2699026.2699128.
- Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage (2013): A fistful of bitcoins: characterizing pay-ments among men with no names, in: Proceedings of the 2013 conference on Internet meas-urement conference (IMC '13) Association for Computing Machinery, New York, NY, USA, 127–140. https://doi.org/10.1145/2504730.2504747.
- Reid, Fergal and Martin Harrigan (2012): An Analysis of Anonymity in the Bitcoin System, in Proc. IEEE 3rd Int. Conf. Privacy Secur., Amsterdam, Netherlands, Oct. 2012, pp. 16–20.
- Victor, Friedhelm (2020): Address Clustering Heuristics for Ethereum. In: Bonneau, J., Heninger, N. (eds) Financial Cryptography and Data Security. FC 2020. Lecture Notes in Computer Science, Vol. 12059, Springer, DOI: 10.1007/978-3-030-51280-4_33.
- Yin, Hao Hua Sun, Klaus Langenheldt, Mikkel Harlev, Raghava Rao Mukkamala and Ravi Vatrapu (2019): Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain, Journal of Management Information Systems, 36:1, pp. 37-73, DOI: 10.1080/07421222.2018.1550550.