EUROPEAN CENTRAL BANK
EUROSYSTEM

BANK OF JAPAN

12 February 2020

STELLA

ECB/BOJ joint research project on distributed ledger technologies

Balancing confidentiality and auditability in a distributed ledger environment

Motivation of Stella phase 4

There has been a growing interest in developing settlement assets, such as stablecoins, central bank digital currency (CBDC) or other types of digital assets, which could be used on platforms based on distributed ledger technologies (DLT). Transactions on DLT networks arguably raise questions on privacy since participating entities own nodes and share transaction information amongst themselves. So-called privacy-enhancing technologies/techniques (PETs) have emerged to address these questions, focusing for example on limiting access to information by third parties. At the same time, there need to be arrangements, including third parties which can check transactions (“auditor[s]”), in place on DLT-based payment and settlement systems to ensure accountability.

Challenges arise when the auditor checks transactions that are made confidential using PETs. Stella phase 4 therefore analyses how confidentiality and auditability could be balanced in a distributed ledger environment. Through conceptual studies and practical experimentation, it explores how PETs would ensure confidentiality, as well as the arrangements that accommodate the auditing of transactions in DLT-based financial market infrastructures (FMI).

Main results of Stella phase 4

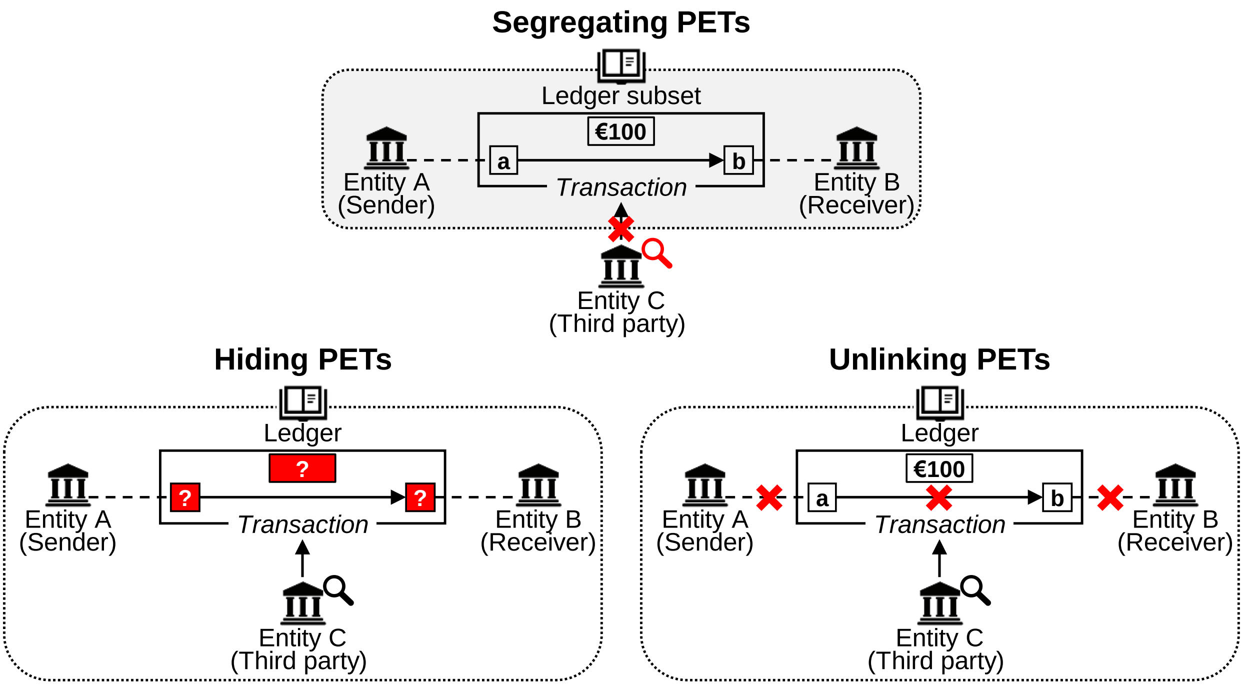
Stella phase 4 outlines the fundamental features for ensuring the confidentiality of transactions, and assesses whether auditing could be done effectively even when confidentiality is ensured. The results can be used as a starting point for choosing PETs and designing auditing processes for transactions.

Three categories of PETs

PETs can be divided into three categories based on the underlying concepts for making transaction information confidential towards third parties (Figure A).

- **Segregating** PETs ensure that each participant can only view a subset of all transactions conducted in the network.
- **Hiding** PETs make use of cryptographic techniques to prevent third parties from interpreting transaction details.
- **Unlinking** PETs make it difficult for third parties to determine transacting relationships from the sender/receiver information recorded on the ledger.

Figure A – Three categories of PETs

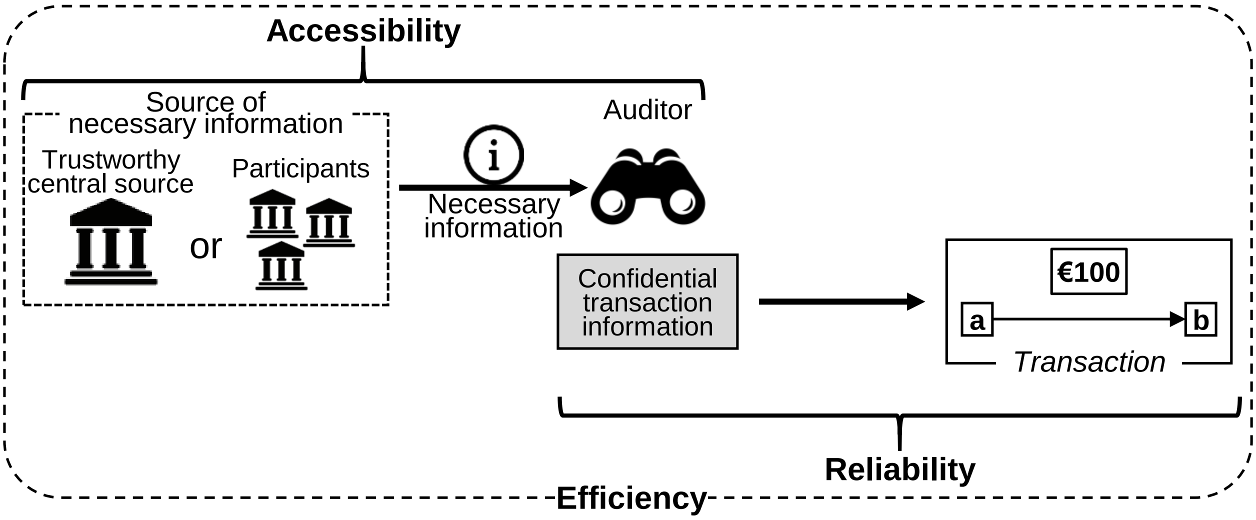


Three perspectives for auditability

Stella phase 4 proposes three key perspectives for assessing the auditability of each PET setup (Figure B).

- **Accessibility** to the necessary information: whether the auditor can obtain with certainty the information it needs to conduct auditing activities.
- **Reliability** of the obtained information: whether the auditor can interpret confidential transaction information with certainty using the obtained information.
- **Efficiency** of the auditing process: whether the auditing process could be conducted in a manner efficient enough for it to be feasible.

Figure B – Concepts of auditing processes and three perspectives


Accessibility
Source of necessary information
Trustworthy central source
or
Participants
Necessary information
Auditor
Confidential transaction information
€100
a
b
Transaction
Reliability
Efficiency

Effective auditing can be achieved when the auditor receives necessary information from participants in such a way that the three perspectives above are accommodated. The existence of trustworthy central sources of information in auditing processes would be beneficial for effective auditing, since it would ensure all three perspectives at the same time without requiring cooperation from the participants. However, despite its contribution to effective auditing, the presence of such sources could present single point of failure risks for the network.

Background on Project Stella

Since its inception in December 2016, Project Stella, a joint research project of the European Central Bank (ECB) and the Bank of Japan (BOJ), has contributed to the ongoing debate via experimental work and conceptual studies exploring the opportunities and challenges of DLT for FMI.[1] This work has resulted in three previous reports. Phase 1, published in September 2017[2], analysed the processing of large-value payments using DLT; phase 2, published in March 2018[3], investigated securities delivery versus payment in a DLT environment; and phase 3, published in June 2019[4], considered whether cross-border payments could potentially be improved, especially in terms of safety, by using DLT-related technologies.

[1] The analysis and experimental results presented in Project Stella are not geared towards replacing or complementing existing arrangements, which include central bank-operated payment systems. Moreover, legal and regulatory aspects are outside the scope of the project.

[2] *Payment systems: liquidity saving mechanisms in a distributed ledger environment*, ECB and BOJ, September 2017.

[3] *Securities settlement systems: delivery-versus-payment in a distributed ledger environment*, ECB and BOJ, March 2018.

[4] *Synchronised cross-border payments*, ECB and BOJ, June 2019.